O QUE ESTÁ EM JOGO NO DEBATE SOBRE **DADOS PESSOAIS** NO BRASIL?

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

INTERNET LAB pesquisa em direito e tecnologia

Também disponível em **www.internetlab.org.br**

O QUE ESTÁ EM JOGO NO DEBATE SOBRE **DADOS PESSOAIS** NO BRASIL?

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

***

EQUIPE INSTITUCIONAL **Diretor Presidente** Dennys Antonialli **Diretor** Francisco Brito Cruz **Diretora** Mariana Giorgetti Valente / EQUIPE DO PROJETO **Líder de projeto** Francisco Brito Cruz **Líder de projeto** Dennys Antonialli **Pesquisador** Bruno Bioni **Estagiário de pesquisa** Jonas Coelho Marchezan **Estagiário de pesquisa** Maike Wile dos Santos **Estagiário de pesquisa** Pedro Marques Neto **Estagiária de pesquisa** Beatriz Kira **Estagiária de pesquisa** Fabiane Midori Nakagawa

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2016.

INTERNETLAB / Rua Augusta, 2690, Galeria Ouro Fino, Loja 326 / www.internetlab.org.br

O QUE ESTÁ EM JOGO NO DEBATE SOBRE **DADOS PESSOAIS** NO BRASIL?

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

/SUMÁRIO

Equipe envolvida neste projeto

Líderes de projeto

FRANCISCO CARVALHO DE BRITO CRUZ / Doutorando em Filosofia e Teoria Geral do Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP), com mestrado (2015) e graduação (2011) pela mesma universidade. Durante o curso, foi bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica. Foi pesquisador visitante (2013) no *Center for Study of Law and Society* da Universidade da Califórnia – Berkeley, por meio de programa de intercâmbio da Rede de Pesquisa Empírica em Direito (REED). Foi ganhador do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). É advogado com atuação nas áreas de direito digital, propriedade intelectual, imprensa e direito do consumidor. Foi fundador e coordenador do Núcleo de Direito, Internet e Sociedade (NDIS FDUSP) entre 2012 e 2014. Atualmente é diretor do InternetLab.

DENNYS ANTONIALLI / Doutorando em direito constitucional pela Universidade de São Paulo, com graduação em direito pela mesma universidade (2008), mestrado em direito pela Universidade de Stanford (JSM, 2011) e mestrado profissional em "*Law and Business*", conjuntamente oferecido pela *Bucerius Law School* e pela WHU *Otto Beisheim School of Management* (MLB, 2010). Atuou junto à equipe de políticas públicas em tecnologia e direitos civis na *American Civil Liberties Union of Northern California* (ACLU/NC) e como consultor jurídico do "*Timor Leste Legal Education Project*", da *Stanford Law School/Asia Foundation*. Foi ganhador do 1º lugar do *Steven M. Block Civil Liberties Award* da *Stanford Law School* (2011) e do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). Foi pesquisador do *Alexander von Humboldt Institute for Internet and Society (*Berlim) e participou do *Summer Doctoral Program* do *Oxford Internet Institute*. Fundador do Núcleo de Direito, Internet e Sociedade da FDUSP (NDIS), atualmente é Visiting Scholar na Stanford Law School e diretor presidente do InternetLab.

Pesquisador

BRUNO RICARDO BIONI / Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (2016), pós-graduado em Direito Civil e Consumidor pela Escola Paulista de Direito (2013) e graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (2012). Foi study visitor do Departamento de Proteção de Dados Pessoais do Conselho da Europa (2015) e pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa (2014-2015). Atualmente é pesquisador do Grupo de Políticas Públicas para o Acesso à Informação/GPoPAI da Universidade de São Paulo (Projeto Privacidade e Vigilância no Brasil) e advogado do Núcleo de Informação e Coordenação do Ponto Br/NIC.br.

Estagiárixs de pesquisa

JONAS COELHO MARCHEZAN / Graduando em Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Voluntário na Equipe Societária do Departamento Jurídico da ONG "*Un Techo para Mi Pais* – Teto Brasil".

MAIKE WILE DOS SANTOS / Graduando em Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Fez parte da Escola de Formação na Sociedade Brasileira de Direito Público – SBDP (2014). Foi monitor-bolsista do Programa de Estímulo ao Ensino de Graduação – PEEG da disciplina Instituições de Direito para Economistas, na FEA (2013), e pesquisador-bolsista do Programa Ensinar com Pesquisa no Núcleo de Direito, Internet e Sociedade – NDIS (2014), ambos vinculados à USP. Atualmente é membro do Centro de Análise e Pesquisa em Educação Jurídica – CAPEJur, vinculado ao Departamento de Filosofia e Teoria Geral do Direito da FDUSP, e estagiário de pesquisa no InternetLab.

BEATRIZ KIRA / Graduada em Direito pela Universidade de São Paulo (FDUSP). Foi bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica. Realizou intercâmbio acadêmico na Ludwig-Maximilians-Universität München para realização do "Aufbaustudium in den Grundzügen des Deutschen Rechts" – curso preparatório para o LL.M. em direito alemão -, período em que foi bolsista do Deutscher Akademischer Austauschdienst (DAAD). É assistente de pesquisa da Rede de Pesquisa Empírica em Direito (REED) e pesquisadora do InternetLab.

FABIANE MIDORI SOUSA NAKAGAWA / Graduanda em Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP), onde participa do programa de duplo-diploma em Direito oferecido pela Université Jean Moulin – Lyon III. Realizou intercâmbio acadêmico na Ludwig-Maximilians-Universität München para realização do "Aufbaustudium in den Grundzügen des Deutschen Rechts" – curso preparatório para o LL.M. em direito alemão -, período em que foi bolsista do Deutscher Akademischer Austauschdienst (DAAD) (2015-2016). Foi diretora do Núcleo de Direito Internacional do Largo São Francisco (NEI) na FDUSP (2014). Atualmente é estagiária de pesquisa no InternetLab.

1. INTRODUÇÃO

1.1. Anteprojeto de lei de proteção de dados pessoais: contexto

A consulta pública sobre o anteprojeto de Lei de Proteção de Dados Pessoais foi realizada pela Secretaria Nacional do Consumidor (SENACON) em conjunto com a Secretaria de Assuntos Legislativos (SAL) dentro do escopo do projeto "Pensando o Direito" do Ministério da Justiça. Esse projeto promove, desde 2007, maior participação da sociedade na elaboração de leis e regulamentos no Brasil e busca, dessa forma, criar normas mais efetivas e conectadas com a realidade atual e as demandas dos cidadãos.

A consulta pública sobre a qual se debruça este relatório foi realizada entre 28 de janeiro e 05 de julho de 2015 e girou em torno dos 52 artigos do texto proposto do anteprojeto. As várias contribuições dos setores público e privado, academia, cidadãos e organizações não-governamentais foram utilizadas pelo Ministério da Justiça para elaboração da nova versão do Anteprojeto de Lei de Proteção de Dados pessoais, apresentada no dia 20 de outubro de 2015.

O texto submetido à consulta pública já havia sido reformulado pelo Ministério da Justiça, que voltou a priorizar o assunto após as denúncias de Edward Snowden em 2013. O esforço para aprovar uma legislação geral de proteção de dados pessoais no Brasil não é injustificado: mais de cem países possuem legislações nesse sentido ao redor do mundo.[1] Enquanto a União Europeia, desde 2012, já discute a reforma do seu marco regulatório em relação à matéria - a Diretiva 95/46/EC, que estabeleceu parâmetros para as legislações nacionais de proteção de dados dos países membros e que está em vigor desde 1995 -, o Brasil segue sem regulamentação específica.

Além de gerar insegurança jurídica, esse atraso exclui o Brasil, por exemplo, da lista de países considerados como adequados pela União Europeia para atuar como destinatários de dados pessoais de cidadãos europeus, impedindo, portanto, que esses dados possam ser transferidos a empresas brasileiras em algumas circunstâncias.

Ao mesmo tempo em que a discussão avança no Ministério da Justiça, iniciativas concomitantes também estão sendo discutidas no âmbito do Poder Legislativo, como é o caso dos projetos de lei nº 4060/2012, de autoria do deputado Milton Monti (PR-SP) e nº 181/2014, de autoria do ex-senador Vital do Rêgo (PMSB-PB).

1.3. O debate de 2015: formas de participação

A plataforma da consulta oferecia três possibilidades para contribuir: *(i)* comentário no texto da lei, *(ii)* comentário por eixo temático, e *(iii)* envio de contribuição via PDF. O primeiro

[1] Graham Greenleaf. Global Data Privacy Laws: 109 Countries, with European Laws Now a Minority, *133 Privacy Laws & Business International Report, February 2015* , disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529

formato possibilitava que os participantes interagissem com cada um dos dispositivos da lei, o que favorecia o diálogo e a contraposição de ideias, uma vez que os comentários já feitos eram exibidos a todos os participantes. Por outro lado, como o texto da lei estava organizado pela ordem dos artigos, notamos uma maior concentração de contribuições nos dispositivos do início do anteprojeto, em detrimento dos dispositivos do final do texto.

O segundo formato permitia comentários por eixos temáticos, mas foi pouco utilizado, uma vez que a plataforma não deixava clara esta possibilidade. Durante o período de debate público, os poucos comentários recebidos se tornaram inacessíveis, o que levou à opção metodológica de não considerá-los na elaboração desta análise.

Por fim, havia a possibilidade de envio de contribuições em arquivos PDFs. Este formato viabilizava contribuições maiores e mais complexas, sem limitação de espaço e sem se limitar a comentar especificamente um dispositivo em específico do APL. Nesse caso, a interação entre os participantes ficou limitada, pois não era possível comentar diretamente o texto dos arquivos.

1.4. Qual foi o papel do InternetLab?

Ocupando o papel de uma entidade acadêmica, o InternetLab desenvolveu uma metodologia de acompanhamento e sistematização das contribuições enviadas para a consulta pública. Enquanto a consulta esteve aberta, publicamos boletins semanais com as principais contribuições ou discussões que ocorreram na plataforma. Buscamos destrinchar temas complexos que surgiram durante esses processos, inclusive por meio de entrevistas com pesquisadores especialistas. O objetivo foi dar visibilidade a esse momento importante para o estabelecimento de um marco regulatório brasileiro de proteção dos dados pessoais. Buscamos, assim, fomentar a participação e possibilitar a entrada de outros interessados na discussão por meio da divulgação de informações concisas e organizadas sobre as pautas e principais debates na plataforma.

Este relatório apresenta o resultado final de nossa análise e acompanhamento da plataforma, sistematizando as contribuições e produzindo um panorama com os principais argumentos, além de trazer a nova redação do anteprojeto, apresentada pelo Ministério da Justiça em 20 de outubro de 2015.

2. METODOLOGIA

Foram analisadas todas as contribuições enviadas ao Ministério da Justiça por meio da plataforma "Pensando o Direito" durante todo o período da consulta, que aconteceu entre os dias 28 de janeiro e 05 de julho de 2015.

O debate girou em torno da redação proposta pelo Ministério (52 artigos divididos em 13 eixos temáticos). Os participantes eram livres para fazer comentários em cada dispositivo do anteprojeto (artigos, parágrafos, incisos e alíneas) por meio da ferramenta fornecida pela plataforma, apresentar contribuições por eixos temáticos, ou, caso preferissem, enviar a íntegra de sua proposta em arquivos PDFs que se tornavam visíveis e disponíveis para consulta do público em geral. Como os (poucos) comentários feitos por eixo temático e não por artigo iam se tornando posteriormente inacessíveis na plataforma, eles não foram considerados na elaboração deste relatório. Os comentários feitos por meio de documentos em PDF foram organizados conforme os dispositivos que compõem a redação do anteprojeto.

2.1. Como foi feita a análise?

Da totalidade das contribuições, foram suprimidas do relatório aquelas que *(i)* não possuíam relação temática com o tema em pauta; e *(ii)* que sugeriam tão somente o remanejamento dos dispositivos do anteprojeto para "facilitar a interpretação" ou em benefício da "melhor técnica legislativa". Apesar da importância desses tipos de contribuição, nosso relatório foi pautado na reunião dos distintos argumentos concernentes aos vários temas da proteção de dados pessoais e não na melhor organização do futuro projeto de lei.

A partir desse recorte, buscamos identificar, em cada uma das contribuições, as teses e argumentos defendidos, assim como relacioná-los com os agentes que atuaram na plataforma. Além disso, identificamos uma temática central em cada um dos artigos do anteprojeto e procuramos agrupar as teses e argumentos das contribuições de acordo com estas temáticas. Temas que se repetiram e se tornaram muito complexos foram realocados no relatório, de modo que algumas discussões recorrentes foram concentradas para análise em único artigo, com o objetivo de facilitar a compreensão.

Além disso, sugestões de exclusão ou alteração de dispositivos ao longo do texto justificadas por posições contrárias à criação de novo órgão competente foram, para evitar repetição, consolidadas em uma única manifestação que consta na seção do relatório dedicada ao órgão competente.

As contribuições foram então divididas em três categorias:

1) Questões Controversas

Essa categoria diz respeito àquelas contribuições que foram efetivamente debatidas, apresentando posições conflitantes. É importante ressaltar que, nesses casos, não necessariamente essas contribuições foram feitas no mesmo dispositivo. O critério para organizá-las dessa forma foi que guardassem forte relação temática.

2) Propostas Avulsas

Essa categoria diz respeito àquelas contribuições que não encontraram contraposição direta no debate. Cabe observar que nem todas as propostas esparsas analisadas integram este relatório, tanto em função da aplicação dos critérios de exclusão já mencionados, quanto por algumas terem sido resumidas para melhor compor o resultado.

3) Sugestões de redação

Essa categoria elencou sugestões de redação feitas pelos participantes. Na maioria das vezes, essas sugestões tiveram correspondência com alguma das respostas de questão controversa ou proposta avulsa elencada. Em alguns casos, entretanto, foram sugestões de redação isoladas, sem maiores considerações temáticas.

2.2. Comentários da equipe do InternetLab

Este relatório também conta com comentários feitos pela equipe do InternetLab para aprofundamento contextual de discussões travadas na plataforma.

2.3. O que esperar do presente relatório?

O relatório busca realizar uma descrição do processo de consulta, mapeando os pontos em debate, os principais argumentos levantados e os agentes engajados, para que, a partir desse trabalho analítico, fique mais fácil avaliar as propostas realizadas e as opções legislativas que forem feitas. Não há aqui a pretensão de apresentar exaustivamente todos os posicionamentos do debate, mas espera-se que o relatório sirva de guia para estudos aprofundados sobre cada um dos temas expostos. Destarte, espera-se oferecer subsídios à construção da futura Lei de Proteção de Dados Pessoais, mostrando até que ponto a nova versão do anteprojeto, disponibilizada pelo Ministério da Justiça em 20 de outubro de 2015, foi permeável ao debate travado na plataforma.

2.4. Licença de uso de conteúdo

3. MAPA DE ARGUMENTOS E PROPOSTAS GERAIS

3.1. Como deve ser o órgão responsável pela aplicação da lei de proteção de dados pessoais?

A discussão a seguir trata da proposta de criação de um órgão competente para fiscalizar a aplicação da lei de proteção de dados pessoais, o que envolve debater fatores como sua composição, arranjo institucional e forma de financiamento. Contribuições que dizem respeito ao maior ou menor escopo de atuação e poder desse órgão estão espalhadas ao longo do relatório nos dispositivos que mencionam o órgão e suas atribuições.

Uma análise abrangente dos comentários dos participantes revela certa coesão quanto às características gerais que devem pautar a criação do órgão. Tais características têm proximidade com o formato de autoridades de garantia de dados pessoais europeias. Segundo a maioria dos participantes, a autoridade deve ser **composta por funcionários especializados tecnicamente**, deve ter **independência** tanto financeira quanto decisória e deve ser **única**, centralizada, tendo suas atividades empreendidas em âmbito federal. Outra característica que foi apontada como necessária é a **permeabilidade com relação a todos os setores da sociedade com interesse na regulação da proteção de dados pessoais**, sendo que alguns participantes apontaram a necessidade de criação de um conselho consultivo (*ABEMD* e *CTS-FGV*).

Entretanto, essa visão geral sobre o órgão não é unânime. O formato "europeu" recebeu uma série de críticas ao longo do debate. Alguns participantes **não são nem mesmo a favor da criação** de um novo órgão para cuidar do cumprimento da lei:

> "Não é necessária a criação de órgão competente específico, consideramos que já existem no sistema jurídico brasileiro órgãos com competência para fiscalizar a aplicação das leis vigentes que tratam de dados pessoais, incluindo o Ministério Público"
> **Autores da proposta**: *SindiTeleBrasil*, *Vivo*, *Claro*[2] e *GSMA*

A ideia de que o órgão seja único e de competência federal **também não é aceita unanimemente**. O *GPoPAI* sugeriu a seguinte redação do texto legal:

> *"***Sugestão de redação**: '*Art. 52. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa'.* (*GPoPAI*)

[2] Apesar de ser contra a criação do órgão pela lei, a *Claro* aponta algumas características que considera necessárias para um futuro órgão, caso ele exista. Na opinião da empresa ele deve agir de forma imparcial e independente, possuir capacidade e composição técnica e não vir a aumentar a carga burocrática de procedimentos e exigências administrativas para a condução dos negócios envolvendo dados pessoais.

Outro ponto em que houve discordância entre os participantes do debate foi **o financiamento do órgão competente**. Ocorreu um embate de opiniões quanto ao uso dos recursos oriundos das multas aplicadas pelo órgão. A *Proteste* sugeriu o uso dos recursos à semelhança do que é feito na Espanha (onde o órgão de aplicação da lei de proteção de dados é sustentado pelas multas que ele mesmo aplica), enquanto *ITI*, *Brasscom* e *ABRANET* foram expressamente contrários a esse modelo.

Abaixo foram compiladas as diferentes contribuições dos participantes do debate acerca do formato do órgão competente para a aplicação da lei de proteção de dados pessoais.

Propostas avulsas para a regulação deste tema:

(A) O órgão deve conter um conselho consultivo e deliberativo multissetorial.

"*Entendemos que é de fundamental importância que o órgão competente conte com um conselho Consultivo e Deliberativo com formação paritária, envolvendo membros do governo, sociedade civil e setor empresarial (sempre com definição prévia de critérios técnicos mínimos de qualificação profissional).* "

Autores da proposta: *ABEMD.*

(B) Deve haver apenas um órgão competente para a aplicação da lei.

"*Acreditamos que o ideal é que apenas UM órgão seja responsável pela fiscalização e outras atividades dispostas nesse Anteprojeto de Lei. Dessa forma, haverá consistência nas interpretações e certeza regulatória. Além disso, também somos a favor da criação de um órgão independente com pessoas especializadas e preparadas para atender as expectativas".*

Autor da proposta: *Câmara BR***.**

(C) O órgão deve ser único e com orçamento próprio, devendo investigar, intervir e poder ser consultado.

"*Quanto ao órgão competente, a RELX é favorável à existência de um órgão competente único com orçamento e funcionários próprios. Ele deveria ser criado simultaneamente com essa estrutura de privacidade. Ele terá capacidade de investigar e intervir, e possuirá poder consultivo.*

Tal poder é importante no auxílio de empresas, pois o órgão terá o conhecimento apropriado para interpretar a lei de proteção de dados pessoais em cenários diferentes. Por fim, esse órgão também servirá como ombudsman, investigando reclamações individuais contra a má-administração de empresas, bem como de autoridades públicas".

Autor da proposta: *RELX Group.*

(D) Pode ser criada uma autarquia ou um sistema nacional de proteção de dados pessoais.

"*Tendo em vista a experiência em diversos países europeus e as dificuldades em escolher entre as*

opções jurídico-administrativas para a criação da autoridade em questão, sugere-se que as obrigações e atribuições da autoridade dispostas ao longo do APL sejam sistematizadas e complementadas em um capítulo específico dedicado à criação da autoridade de proteção de dados.

Através da experiência europeia, podemos aferir que a autoridade brasileira deverá: (i) ter natureza jurídica de direito público; (ii) ser independente, muito embora tal característica tenha diferentes formas dependendo do arranjo administrativo escolhido; e (iii) exerça diversos poderes, inclusive poderes de polícia.

Tendo em vista as características elencadas acima, destacam-se dois arranjos administrativos possíveis: uma ***autarquia*** *ou um* ***sistema nacional de proteção de dados pessoais****.*

Autarquia. *A criação de uma autarquia se justificaria em função de sua (i) natureza jurídica de direito público; (ii) independência e autonomia; e (iii) possibilidade de exercer poderes de polícia. De acordo com o descrito neste documento, este modelo se aproximaria do modelo de referência, o modelo usado nos países da União Europeia.*

É necessário lembrar, contudo, que o poder de uma autarquia não pode ser oponível em relação aos órgãos que compõem a administração pública direta ou indireta, uma limitação de um modelo institucional baseado em uma autarquia. Assim, necessitamos pensar na em mecanismos de proteção de dados pessoais que também possam ser oponíveis a órgãos que compõem a administração pública.

Por fim, ressaltamos que caso seja criada uma autarquia, será necessária a aprovação de uma lei não apenas para a criação da autoridade em questão, mas também seria necessária uma lei caso seja necessário extingui-la".

Sistema nacional de proteção de dados pessoais. *A semelhança dos sistemas já existentes no Brasil: Sistema Nacional de Defesa do Consumidor (SNDC), como o Sistema Brasileiro de Defesa da Concorrência (SBDC), e o Sistema Nacional de Proteção e Defesa Civil (SINPDEC).*

A criação de um sistema nacional de proteção de dados seria uma forma de permitir que diferentes objetivos sejam cumpridos. Por exemplo, que a futura lei de proteção de dados assim como as normas dela decorrentes sejam oponíveis a entes públicos e privados. Além disso, permitiria que a elaboração de normas de forma a levar em consideração diferentes aspectos técnicos e políticos envolvidos. Assim, é possível que seja desenvolvido um sistema que conte com uma autarquia e um órgão da administração direta. Desta forma, as diferentes entidades trabalhariam de forma a coordenar a política pública e a regulação da proteção de dados.

Por fim, cabe dizer que Independentemente do modelo adotado para o "órgão competente" para a proteção dos dados no Brasil, tal composição institucional poderia ser complementada pela formação de um conselho - ou outra forma de colaboração - composto por membros da sociedade civil, da academia, do setor privado e do setor público".

Autor da proposta: *CTS-FGV.*

(E) O órgão competente deve ter o formato de agência reguladora.

"Quanto a autoridade reguladora, a melhor solução seria a criação de uma agência de proteção de dados, no formato de uma agência reguladora, com independência financeira e administrativa e com mandato fixo para os seus diretores. Essa agência, futuramente, poderia também englobar competências relacionadas a outros temas, como a Lei de Acesso à Informação. Esse, aliás, foi o modelo adotado por todos os países membros da União Europeia". (*ITS-Rio*)

"É importante reforçar que as atribuições que a lei concede ao órgão competente não devem recair

sobre um órgão já existente. É de extrema importância a criação de um órgão federal autônomo, específico e exclusivo para fazer cumprir, da melhor maneira, a lei de proteção de dados, em razão da complexidade de referido tema.

Fazendo um paralelo com o direito brasileiro, esse órgão competente poderia seguir um modelo de agencia reguladora, uma autarquia com autonomia e independência, formada por pessoas com conhecimento técnico". (*Câmara BR*)

Autor da proposta: *ITS-Rio* e *Câmara BR.*

(F) O órgão competente deve ser único, independente e dotado de orçamento operacional que não inclua as multas cobradas pelas violações da presente lei.

"Recomenda-se que a execução da lei seja destinada a um único e independente órgão competente. Ressalta-se também que a criação de um novo órgão independente, dotado de seu próprio orçamento operacional, não deveria incluir as multas cobradas pelas violações à lei como parte desse orçamento operacional—essa situação cria um incentivo a distorções". (*ITI*)

"A exemplo do que já aconteceu com vários países ao redor do mundo, a lei de proteção de dados pessoais deve ser acompanhada da criação de uma autoridade de proteção de dados, esta terá a incumbência de trabalhar pela aplicação da lei e de realizar interpretações técnico-jurídicas acerca de seus dispositivos de forma a garantir um ambiente com segurança jurídica.

Esta autoridade deverá ser federal e independente, ressalta-se também que o orçamento operacional do órgão deve ser autônomo, sem incluir eventuais multas impostas em decorrência de violações à Lei, a fim que não haja um incentivo na aplicação exacerbada desse instrumento e que caso isto ocorra, suas decorrências sejam destinadas ao combate de crimes digitais, a educação para utilização consciente da internet e a formação de profissionais, tão necessária nesta nova economia". (*Brasscom*)

Autor da proposta: *ITI* e *Brasscom.*

(G) O órgão deve adotar participação multissetorial.

Sugere que o órgão adote participação multissetorial. Como parâmetros, sugere que seja composto por representantes da União, do setor empresarial e industrial, da comunidade científica e da sociedade civil organizada, com competência para propor diretrizes e recomendações técnicas e opinar sobre as propostas de políticas governamentais na área de atuação do órgão.

Autor da proposta: *CNI*.

(H) A lei deve prever a criação do órgão competente, definindo seus recursos, competência e autonomia.

O projeto deveria prever o órgão competente responsável pela proteção de dados, bem como definir seus recursos, competências e autonomia. A criação deste órgão é essencial à efetividade desta lei. Sem ele, restam dúvidas sobre o real comprometimento do Brasil com a proteção de dados pessoais e a privacidade.

"Entendemos que o anteprojeto de lei deve definir qual será esse órgão competente, de forma a se evitar insegurança jurídica e para que a sociedade saiba quem terá o papel de interpretar, fiscalizar

e fazer cumprir a lei" (*IAB*)

Autor da proposta: *Privacy International* e *IAB.*

(I) A vigência da lei deve ser iniciada somente um ano após a criação do órgão competente.

"Sugere-se que o projeto de lei determine a sua entrada em vigor para o período mínimo de um ano após a criação do órgão competente. É importante que a data de implementação das provisões desta regulamentação esteja atrelada a criação de uma autoridade competente, funcional, independente e apropriadamente financiada".

Autor da proposta: *US Business Council.*

(J) O órgão deve ser criado como um departamento dentro do Ministério da Justiça e antes da vigência da lei.

"O anteprojeto deveria definir o órgão competente em seu próprio texto, bem como definir que sua criação ocorra antes da entrada em vigor da lei. Na opinião da Sky, o órgão competente dever ser um órgão de nível federal para garantir tratamento consistente nacionalmente de questões de proteção dedados, em vez de vários regulamentos estaduais.

A Sky também acredita que o órgão competente deveria ser criado como um departamento dentro do Ministério da Justiça, especialmente porque a proteção de dados deveria estar dentro da capacidade institucional do Ministério".

Autor da proposta: *Sky.*

(K) O órgão competente deve ter independência funcional na linha da Carta de Direitos Fundamentais da União Europeia.

"O 'órgão competente', referenciado 34 vezes no APL, deva ter assegurado a sua independência funcional, além de uma gama de poderes que torna viável a sua atuação. Deve-se afirmar, na linha da Carta de Direitos Fundamentais da União Europeia, a independência desse órgão, retomando a primeira versão do APL em que os seus diversos poderes eram elencados. Para isso, sugere uma série de alterações no capítulo VIII".

Autor da proposta: *GPoPAI.*

(L) A lei deverá criar uma autoridade independente de proteção de dados pessoais – nos moldes europeus – que tenha papel de regulação do setor público e privado.

"*A lei deve prever uma autoridade independente para fiscalizar a aplicação das suas disposições. Para real aplicação de todo o previsto na nossa futura lei de proteção de dados pessoais, bem como para solucionar questões em que o estado da tecnologia só nos permite avaliar caso a caso, torna-se indispensável que, nos moldes europeus, a legislação brasileira estabeleça também a criação de uma autoridade independente de proteção de dados pessoais.*

Tal autoridade teria o papel de regulação e aplicação de sanções, não só apenas às pessoas jurídicas de direito privado, mas também à agentes públicos. Se perpassarmos vários dos comentários desta consulta pública, torna-se evidente que muitas das previsões legais apenas se completam com a existência de tal autoridade, sendo que a não previsão de tal órgão é capaz de esvaziar e eficácia de

grande parte das previsões legais desta proposta de lei".

Autora da proposta: *Joana Varon.*

(M) A lei deverá criar uma autoridade federal de proteção de dados técnica e independente.

"Sugerimos que - tendo em vista referência internacional - o projeto de lei proponha a criação de uma autoridade de proteção de dados, de nível federal, como um órgão técnico e independente, com o intuito de supervisionar a implementação e aplicação de um regramento tão importante para o estabelecimento dos direitos dos cidadãos brasileiros na era digital".

Autor da proposta: *Cisco*.

(N) O órgão competente deverá ser uma autoridade com composição plural, com capacidade de análise técnica e autônoma.

"*Sugerimos que a estruturação de uma autoridade paute-se pelos seguintes aspectos: (i) membros escolhidos com base em múltiplas visões das questões de privacidade, com formação técnica prevalecendo sobre a política; (ii) capacidade de análise holística da proteção de dados, levando em conta os impactos na inovação, na economia, nas relações empresariais, internacionais e de consumo, e nas questões concorrenciais. (iii) Autonomia e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade*".

Autor da proposta: *ABRANET*.

(O) O órgão competente deve ter estrutura orçamentária baseada no exemplo espanhol.

"É necessário que se inclua na lei diretrizes para a criação de órgão de natureza pública com competência para regulamentar, fiscalizar e aplicar sanções nos casos de descumprimento da lei. Neste sentido, entendemos que, ainda em caráter ilustrativo, o modelo adotado pela Espanha pode servir de parâmetro para a criação da autoridade brasileira.

A autoridade espanhola é um organismo com autonomia política e administrativa do Poder Executivo com competência inclusive para fiscalizar arquivos da administração pública, como, por exemplo, a polícia e o Poder Judiciário. Ainda que no caso dos órgãos públicos não haja previsão de sanção, mas a expedição de atos administrativos com a determinação de cumprimento da lei.

O financiamento da agência, com custo de 13 milhões de euros em 2013, se dá por intermédio da arrecadação de multas. Em 2013 foram arrecadados 22 milhões de euros em multas pela agência. O excedente entre o custo de manutenção da agência e o total do valor arrecadado é direcionado para a Fazenda Pública".

Autor da proposta: *Proteste.*

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

CAPÍTULO VIII- SANÇÕES ADMINISTRATIVAS E DA INDEPENDÊNCIA DO ÓRGÃO COMPETENTE

Art. 50. O cumprimento dos direitos e obrigações estabelecidos nesta lei fica sujeito à fiscalização por parte do órgão competente, assegurando-se a sua independência com autonomia administrativa, orçamentária e financeira, cuja estrutura e atribuições serão estabelecidas nos termos do regulamento.

Art. 51. Compete ao órgão competente:

I - zelas pela observância desta lei, de seu regulamento e do seu regimento interno;

II - planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais;

III - editar normas e provimentos sobre matérias de sua competência;

IV - aprovar seu regimento interno;

V - receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;

VI - aplicar, de ofício ou a pedido de parte, conforme o caso, sanções apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;

VII - criar, manter e publicar, para fins de transparência, um registro de bancos de dados pessoais de caráter de categorias e setores que considere relevantes, nos termos do regulamento;

VIII - verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados;

IX - promover o conhecimento entre a população das normas que tratam da matéria e de suas finalidades, bem como das medidas de segurança de dados;

X - vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos de regulamento;

XI - reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros que não contem com este nível adequado.

XII - determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento;

XIII - fomentar a pesquisa acadêmica em torno do tema da proteção de dados pessoais, dada a sua autonomia financeira;

XIV - estabelecer e fiscalizar os padrões técnicos para que os direitos e obrigações previstos nessa lei sejam implementados por meio de medidas técnicas e organizacionais para a proteção dos dados pessoais, levando-se em consideração desde a fase de concepção do produto ou serviços até

a sua execução.

XV - desenvolver outras atividades compatíveis com suas finalidades.

Art. 52. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa.

Art. 53. Sem prejuízo das sanções civis e penais cabíveis e de outras sanções administrativas a serem definidas em normas específicas, as infrações das normas previstas nesta lei ficam sujeitas, conforme o caso, às seguintes sanções administrativas: I, II, III, IV, V, VI, VII, VIII, §§ 1º, 2º, 3º, 4º e 5º do antigo art. 50

3.2. Existem outros temas que não foram tratados no anteprojeto de lei de dados pessoais?

Neste ponto foram compiladas as principais sugestões trazidas durante o debate que não guardam relação direta com nenhum dispositivo do texto disponibilizado. São temas que não foram abordados na versão colocada em consulta, mas que, na visão de certos atores, deveriam ter sido.

Propostas avulsas para a regulação do tema:

(A) A lei deve deixar clara a diferença entre pesquisas de mercado e pesquisas de marketing direto – e deve criar exceções ao primeiro tipo.

"*O anteprojeto não deixa claras as diferenças entre pesquisas de mercado de um lado e pesquisas de marketing direto de outro, a falta dessa distinção gera algumas imprecisões. Ademais, não há no anteprojeto proteção para os agentes que manipulam dados: não há responsabilidade dos titulares de dados pela veracidade e legitimidade dos mesmos. O que no âmbito da pesquisa de mercado pode causar graves distorções nos resultados de pesquisas que tem fins sociais e de planejamento de políticas públicas.*

Por fim, resta dizer que a futura lei deveria flexibilizar alguns direitos dos usuários (Acesso, retificação, cancelamento e oposição) com relação às atividades de pesquisa de mercado, posto que o exercício abusivo desses direitos inviabiliza a metodologia das pesquisas de mercado".

Autor da proposta: *ABEP.*

(B) A lei deve obrigar empresas e organizações a elaborarem estudos de impacto de privacidade quando estas tratarem de dados pessoais sensíveis.

"O anteprojeto deve dispor sobre a obrigação de elaboração de Estudos de Impacto de Privacidade para as pessoas naturais e jurídicas de direito privado, quando estas tratarem dados pessoais sensíveis, e para as pessoas jurídicas de direito público, quando estas tratarem quaisquer tipos de

dados".

Autor da proposta: *Rodrigo Veleda.*

(C) A lei deve impor salvaguardas à disponibilização de dados pessoais para autoridades estatais.

"Lei de proteção de dados deveria impor restrições procedimentais às disposições do Marco Civil que previu a divulgação de dados pessoais às autoridades judiciais e do Ministério Público. Isso porque o MCI estabelece uma forte presunção contra o anonimato e, em certos casos, permite o acesso de autoridades a dados sem crivo judicial.

Tendo em vista os direitos fundamentais em jogo, nos casos de crime contra a honra, a lei deveria prever que para requisitar dados pessoais será necessário: mostrar a probabilidade de sucesso na ação contra o potencial ofensor e mostrar que a identificação do ofensor é necessária para reestabelecer a honra, na falta de meios menos restritivos.

No sistema brasileiro, sempre é dever do provedor de conexão ou aplicação reter certos dados de seus usuários. Ao mesmo tempo, sempre que alguém requisitar em juízo acesso aos dados retidos por um provedor e ter sucesso, o provedor terá que pagar as custas judicias. Daí podemos retirar 3 problemas: (i) provedor é obrigado a pagar as custas mesmo sem ter dado causa à ação, (ii) provedor deverá pagar as custas mesmo tendo agido dentro de seu dever legal de guardar dados e (iii) a pessoa cujo anonimato está em jogo (o potencial ofensor) não tem como participar do processo.

Para neutralizar esses problemas, algumas mudanças procedimentais devem ser feitas. Os provedores não devem ser os únicos a defender a privacidade e a liberdade de expressão no processo, tendo em vista a necessidade de contraditório, o provedor deve ser autorizado a notificar o potencial ofensor sobre o processo e este deve ter tempo suficiente para responder à notificação e defender seu anonimato. Nesse cenário, o provedor reproduziria a resposta à notificação nos autos para a apreciação da corte.

Por fim, mudanças devem ser feitas para que o provedor não figure no polo passivo do processo e não seja responsável pelo pagamento das custas judiciais".

Autor da proposta: *Mariana Cunha e Melo.*

(D) A aplicação da lei de dados pessoais deve ocorrer tanto com o setor público quanto com o privado.

"O anteprojeto deverá também observar a questão da unidade, ou seja, deve ter aplicação para o setor privado, público. Verificamos uma grande disparidade de tratamento entre entes de direito público e os demais, a qual não se justifica quando o que está aqui em questão é a proteção de dados pessoais dos cidadãos brasileiros".

Autor da proposta: *Vivo.*

4. MAPA DE ARGUMENTOS E DE PROPOSTAS SOBRE O TEXTO DO ANTEPROJETO

4.1. Direitos fundamentais tutelados

REDAÇÃO LEVADA A DEBATE

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.

No primeiro artigo do anteprojeto, os participantes opinaram acerca *(i)* dos direitos que devem ser protegidos pela lei; *(ii)* das formas de ampliar a defesa dos cidadãos; e *(iii)* das hipóteses de ampliação do escopo da lei.

4.1.1. Quais direitos que devem ser protegidos pela lei de dados pessoais?

O texto original do anteprojeto faz menção aos direitos da liberdade, intimidade e privacidade. Diante disso, os participantes sugeriram outros direitos e outras formas de redação de forma a melhorar o direcionamento da lei dado pelo artigo 1º.

Propostas avulsas para a regulação deste tema:

(A) A lei deve trazer a proteção à honra e à imagem em seu artigo 1º.

"*É importante ampliar a proteção à honra e a imagem da pessoa uma vez que a Constituição Federal, enquanto diploma normativo magno, erigiu o princípio da dignidade da pessoa humana como um dos fundamentos da nossa República Federativa*".

Autor da proposta: *SindiTeleBrasil* e *Fiesp.*

(B) A lei deve trazer a tutela da igualdade em seu artigo 1º.

Autor da proposta: *Elen.*

(C) A lei deve reformular o uso do termo "intimidade" para "privacidade" e trazer a tutela da liberdade de expressão, da livre iniciativa, defesa do consumidor e desenvolvimento tecnológico do país em seu artigo 1º.

O anteprojeto deve uniformizar o uso do termo "privacidade" ao invés de "intimidade e privacidade da pessoa natural" de forma a se alinhar com o debate nacional e internacional. Além disso "a *lei é muito focada a defesa imediata dos direitos do consumidor e fecha os olhos para o bem estar que é gerado através da livre iniciativa, pela concorrência e pela inovação. Estes fatores trabalham na rede como uma defesa mediata dos direitos dos cidadãos*".

Autor da proposta: *ABRANET.*

(D) A lei deve trazer menção à vulnerabilidade do titular dos dados pessoais em seu artigo 1º.

"Lei deverá fazer menção à vulnerabilidade do titular, de forma que tal pressuposto sirva de guia na interpretação das normas. Anteprojeto deve ser interpretado sob a ótica da relação de assimetria de poder entre responsável pelo tratamento e titular e da vulnerabilidade do titular em seus diversos aspectos (vulnerabilidade técnica, jurídica, política, psíquica e socioeconômica)".

Autor da proposta: *CTS-FGV.*

4.1.2. Deve ser aumentado o escopo de aplicação da lei previsto no artigo 1º?

O artigo 1º dispõe que a lei tem o escopo de tratar dos direitos da pessoa natural. Alguns participantes da consulta sugeriram formas de ampliar e dar mais detalhe a esse escopo.

Propostas avulsas para a regulação deste tema:

(A) Pessoas jurídicas devem estar protegidas pela lei de dados pessoais.

Autor da proposta: *Ana Flávia Fagundes Ferreira* e *gabriellebolina.*

(B) A lei deve tutelar a intimidade de pessoas falecidas.

A sugestão foi feita a partir do exemplo de uma eventual necessidade de punição para a exposição, via aplicativos de troca de mensagens, de imagens de pessoas falecidas.

Autor da proposta: *Larissa Denski Nola.*

(C) A lei deve trazer disposição inicial sobre jurisdição.

Autor da proposta: *Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais previstos na Constituição Federal.

Autor da sugestão: *SindiTeleBrasil*

[MODIFICAÇÃO] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de intimidade, privacidade, honra e imagem da pessoa natural.

Autor da sugestão: *CTS-FGV.*

[MODIFICAÇÃO] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural, atendido o princípio de reconhecimento da vulnerabilidade do titular de dados.

Autor da sugestão: *Câmara BR*

[INCLUSÃO] Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no sistema legislativo brasileiro, relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja signatária.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme assinalam as marcas de edição (em vermelho) no texto original (em azul) abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade~~, intimidade~~ e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4.2. Jurisdição e escopo de aplicação da lei

REDAÇÃO LEVADA A DEBATE

Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:

I – a operação de tratamento seja realizada no território nacional;

II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Esta lei não se aplica aos tratamentos de dados:

I – realizados por pessoa natural para fins exclusivamente pessoais;

II - realizados para fins exclusivamente jornalísticos.

§ 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 nos casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Art. 3º As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.

4.2.1. Quais devem ser as exceções para aplicação da lei de dados pessoais?

O debate trouxe dúvidas quanto à aplicação ou não da lei em algumas hipóteses de tratamento que, por suas características peculiares, poderiam não estar englobadas pelo anteprojeto. O exemplo mais citado de uma dessas hipóteses foi o tratamento não-automatizado de dados: ele também deveria estar incluído no escopo de aplicação da lei?

Propostas avulsas para a regulação deste tema:

(A) A lei deve ser aplicável a tratamentos de dados não-automatizados.

Participantes sugeriram que a limitação do escopo da lei a tratamento automatizados apenas não encontra uma justificativa plausível ou razoável. Não incluir tratamentos não automatizados acabaria por dar margem a criação de nova Lei, específica para esse tipo de tratamento, que poderia não revelar os avanços socialmente já conquistados por este anteprojeto.

Autor da proposta: *ABEMD, CTS-FGV, Margareth, ellen sartori, Magno, Maurício Coeli* e *Eden Grei, Giovanna Carloni*.

(B) A lei não deve ser aplicável a tecnologias desenvolvidas no âmbito da "Internet das coisas" (IoT).

"A tecnologia da Internet das Coisas, por suas características específicas e funcionalidades, não deveria ser discutida no âmbito desse projeto de proteção de dados pessoais ou, alternativamente, no mínimo, deveria estar enquadrada dentro das exceções específicas ao consentimento expresso.

Em muitas situações relacionadas com a IoT, a utilização de consentimento expresso é impraticável. Consideramos que a transparência é a principal medida a ser adotada perante o consumidor, especialmente no que diz respeito ao funcionamento de dispositivos IoT, estimulando o uso consciente desses mecanismos. Certamente o objetivo dessa legislação não é o de impedir o desenvolvimento, mas sim apresentar mecanismos que legitimem o uso de dados conscientemente.

Dessa forma, reforçamos ao legislador brasileiro que leve em consideração considere os riscos de um regime de consentimento de uso de dados altamente restritivo e suas consequências no desenvolvimento econômico do país num futuro próximo". (*Cisco*)

"[R]egras que visam limitações ao tratamento de dados a um mínimo possível e necessidade de consentimento prévio expresso poderiam afetar o desenvolvimento da Internet das coisas, ou, até mesmo, inviabilizar usos inovadores dos dados". (*Brasscom*)

Autor da proposta: *Cisco* e *Brasscom.*

(C) A lei não deve ser aplicável a dados relacionados ao cumprimento de dever legal ou relacionados com a relação de emprego.

"[C]ada vez mais as empresas estão sendo compelidas legalmente a preencher e ceder dados em sistemas como o SPED (Sistema Público de Escrituração Digital) Fiscal, Contábil e Trabalhista e que envolve dados coletados para o exercício da atividade empresarial, de forma que tais situações decorrentes de dever legal imposto devem ser afastadas da incidência da Lei.

Todavia, a exclusão proposta é aplicável tão somente ao tratamento por parte de pessoa jurídica de direito público, não autorizando o tratamento dos dados coletados por parte de qualquer ente privado à margem do disposto na lei. Ou seja, caso o ente privado que realizou a coleta, ou qualquer outro ente privado, venha a demonstrar interesse em desenvolver modelo de negócio a partir do tratamento dos referidos dados, poderá fazê-lo sob a égide e subsunção à lei".

Autor da proposta: *Brasscom.*

(D) A lei não deve ser aplicável às esferas comercial e profissional.

Estender a restrição da lei à esfera comercial ou profissional não corresponde à intenção de proteger as informações mais íntimas do indivíduo, considerando que os dados profissionais devem ser classificados como de natureza pública e pode atentar contra os interesses dos próprios titulares dos dados.

Na realidade, tomando isto como exemplo, no caso do advogado, não se compara falar ao telefone celular particular e falar ao telefone do escritório de advocacia, cuja publicidade, tratamento e cessão não convêm que sejam restritos.

Autor da proposta: *Câmara BR*

(E) A lei deve ser aplicável e voltada também à manutenção da confidencialidade de dados protegidos por sigilo profissional.

Autor da proposta: *Claro.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[INCLUSÃO] Art. 2º, § 2º:

Novo Inciso – relacionados a pessoas naturais, quando se referem a elas em sua qualidade de comerciantes ou profissionais;

Novo inciso – disponíveis ao público ou de conhecimento geral.

Autor da sugestão: *Claro.*

[INCLUSÃO] Art. 2º, § 2º:

Novo Inciso - às informações, dados ou bancos de dados sujeitos a sigilo profissional ou legal, que permanecerão imunes a qualquer tipo de monitoramento ou tratamento por parte de terceiros estranhos ao titular ou ao profissional legítimo detentor.

4.2.2. Jurisdição: quais devem ser os limites da aplicação da lei à coleta de dados pessoais?

Propostas avulsas para a regulação deste tema:

(A) A lei deve ter como critério de aplicabilidade o oferecimento de produtos e serviços ao público nacional.

Os defensores desta proposta afirmam não ser possível identificar a exata localização do usuário no momento em que a coleta de dados se deu. Diante desse fato, o critério estabelecido pela atual redação do parágrafo primeiro e do inciso II do anteprojeto é inviável.

Destarte, a utilização do critério do público foco dos serviços ou produtos parece muito mais efetivo, do ponto de vista das práticas do mercado.

Autor da proposta: *ITI, US Business Council, BSA, ESA, Centre for Information Policy Leadership, Câmara BR, MPA, ITS, GSMA* e *RELX Group.*

(B) A lei não deve ser aplicável a cidadãos brasileiros que estejam vivendo fora do país.

"Propomos nova redação do parágrafo 1º, posto que a atual redação leva a conclusões equivocadas, como por exemplo, a possibilidade de um cidadão brasileiro, que esteja temporariamente vivendo fora do Brasil, poder ter seus dados tratados fora do alcance dessa Lei, mesmo que estejam armazenados no País, o que entendemos não ser razoável".

Autor da proposta: *SindiTeleBrasil* e *Claro.*

(C) A lei não deve criar uma obrigação de verificação do local do titular dos dados no momento da coleta como critério de aplicabilidade.

"*O parágrafo primeiro acaba por criar um ônus adicional aos responsáveis e operadores de ter de verificar se, no momento da coleta, o titular dos dados se encontra no território brasileiro. Isso porque os dados pessoais, muitas vezes, não são coletados diretamente de seu titular, o que torna essa verificação ainda mais complexa*".

Autor da proposta: *ITS-Rio.*

(D) A lei deve se aplicar à coleta de dados feita no território brasileiro apenas quando o responsável por ela também esteja localizado no Brasil.

"Nossa sugestão tem como objetiva limitar o escopo de aplicação da lei, de forma com que a lei só se aplique a casos em que a recolha de dados tiver sido feita no território brasileiro e em que o responsável por essa recolha esteja localizado em território brasileiro.

Tal como está a redação do artigo amplifica muito o escopo de aplicação da lei, podendo se valer até mesmo para empresas com sede fora do Brasil".

Autor da proposta: *Vivo.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, com sede no território nacional, desde que os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] Art. 2º (...) II - Os dados pessoais relacionam-se especificamente a residentes Brasileiros caso tenham sido intencionalmente coletados no território nacional.

Autor da sugestão: *Centre for Information Policy Leadership.*

[MODIFICAÇÃO] Art. 2º A presente Lei impõe obrigações sobre responsáveis com relação às operações de tratamento realizadas por meios totalmente ou parcialmente automatizados direcionadas a indivíduos que residem no Brasil, independentemente do país onde os

responsáveis se encontram e o país onde ocorre o tratamento, conquanto que os dados pessoais a serem processados tenham sido intencionalmente coletados de ou sobre indivíduos no território nacional.

§ 1 Os dados pessoais são considerados como coletados de ou sobre indivíduos no território nacional se os titulares dos dados estiverem localizados no território nacional no momento da coleta

Autor da sugestão: *Claro.*

[MODIFICAÇÃO] Art. 2º (...) II - Os dados pessoais objeto do tratamento tenham sido coletados no território nacional, independente do local de armazenamento.

Autores da sugestão: *Claro e SindiTeleBrasil*

[INCLUSÃO] Art. 2º (...) § 1º Consideram-se coletados no território nacional quaisquer dados pessoais armazenados no Brasil; aqueles disponibilizados pelo titular, quando esse se encontrar em território brasileiro no momento da coleta; e aqueles disponibilizados pelo titular, quando esse se encontrar fora do território brasileiro, à pessoa jurídica com sede no país.

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO E INCLUSÃO] Art. 2º (...) § 4º. Em caso de conflito entre leis, a aplicação da presente lei não excluirá a aplicação de legislação estrangeira, desde que este país possua nível equivalente de proteção para o Brasil

§ 5º A aplicação desta Lei não excluirá ou afastará a lei estrangeira de países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei nas hipóteses de conexão ou conflito de leis no âmbito internacional

4.2.3. Jurisdição: quais devem ser os limites da aplicação da lei ao tratamento de dados pessoais?

Propostas avulsas para a regulação deste tema:

(A) A lei deve ser aplicável apenas na hipótese de o estabelecimento principal do agente de tratamento estar localizado no Brasil.

Proposta de nova redação como forma de forma a evitar conflitos de lei e facilitar o controle da aplicação da lei.

Autor da proposta: *Câmara BR.*

(B) A lei não deve ser aplicável a empresas que tratem de dados de titulares não-brasileiros e que não residam no país – mesmo se o agente de tratamento estiver localizado no Brasil.

A disposição do inciso I do artigo 2º restringiria oportunidades para o Brasil no mercado global de

tratamento de dados. Na atual redação, a lei se aplicaria a empresas sediadas no Brasil que tratam dados de titulares não brasileiros e que não residam no Brasil, o que não seria ideal.

Autor da proposta: *GSMA, Vivo e Centre for Information Policy Leadership.*

(C) A lei deve ser aplicável aos casos em que *(i)* o controlador possua estabelecimento no Brasil responsável pela decisão sobre tratamento de dados; *(ii)* sejam visados pelo tratamento titulares residentes no Brasil; e *(iii)* a coleta seja feita pelo próprio estabelecimento ou em seu nome.

Autor da proposta: *ITI.*

(D) A lei somente deve dispor sobre jurisdição no capítulo sobre transferência internacional de dados.

"Escopo de aplicação da lei deve ser reduzido. Dados oriundos do exterior processados no Brasil e os dados brasileiros processados no exterior, estarão suficientemente garantidos pelas restrições impostas no capítulo V, Transferência Internacional de Dados, não sendo necessário a aplicabilidade de uma segunda legislação".

Autor da proposta: *Brasscom.*

(E) A lei deve abranger também os tratamentos de dados que são apenas parcialmente realizados em território nacional.

Autor da proposta: *ABDTIC.*

(F) A lei deve ser aplicável a empresas que tenham filiais no Brasil.

"A fixação de jurisdição deve levar em conta a presença de filiais ("estabelecimentos" de filiais) de "agentes de tratamento" em território nacional. Deve-se ainda levar em consideração o exemplo da Diretiva 95/46/EC que expande o conceito de "estabelecimento" para além das filiais físicas".

Autora da proposta: *Giovanna Carloni.*

(G) A lei não deve ser aplicável a dados que estejam meramente em trânsito.

Para estes participantes, a lei deveria deve mencionar expressamente que se aplica a dados que estejam meramente em trânsito. Dessa forma, evitar-se-iam conflitos de jurisdições já que, por exemplo, dados coletados fora do Brasil podem acabar eventualmente circulando no território brasileiro.

Autor da proposta: *IAB* e *Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, desde que:

I – o estabelecimento principal esteja localizado no Brasil;

4.2.4. A lei deve se aplicar a tratamentos realizados por pessoa natural para fins exclusivamente pessoais?

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

"*A lei deveria abranger os tratamentos realizados por pessoa natural para fins pessoais, vez que não se sabe se esses fins pessoais serão idôneos*"

Quem defende isso? *Márcia P. Soldate.*

(B) Sim, mas com nova redação.

"*Considerando a necessidade de coibir tratamentos realizados para 'fins dolosos', sugere-se a nova redação*".

Quem defende isso? ABDTIC

(C) Não, desde que o tratamento seja feito dentro de um contexto privado.

"*Sugerimos o acréscimo da expressão "dentro de um contexto privado" para especificar melhor o inciso*".

Quem defende isso? *Câmara BR* e *ABRANET.*

Sugestões de redação:

Autor da sugestão: *Câmara BR* e *ABRANET.*

[MODIFICAÇÃO] Art. 2º § 2º (I) realizados por pessoa natural, dentro de um contexto privado, para fins exclusivamente pessoais.

Autor da sugestão: *ABDTIC.*

[MODIFICAÇÃO] Art. 2º § 2º (I) realizados sem dolo por pessoa natural para fins exclusivamente pessoais.

4.2.5. A lei deve se aplicar a tratamentos realizados para fins exclusivamente jornalísticos?

O inciso II do artigo 2º trata da não-aplicação da lei para tratamentos de dados realizados para fins exclusivamente jornalísticos. Este dispositivo ocasionou uma grande quantidade de questionamentos na plataforma de consulta sobre a real definição de "fins exclusivamente jornalísticos". Os participantes questionavam principalmente o abuso desta abertura legal pela "mídia sensacionalista".

Neste sentido, boa parte dos comentários demandava uma melhor definição do termo. Paralelamente, porém, ocorreu a discussão sobre a procedência ou não da exceção feita pela lei, como se verá:

Respostas controversas coletadas na plataforma de debate:

(A) Sim. A liberdade de imprensa não é um direito absoluto e não justifica a exclusão de dados tratados para fins jornalísticos da lei.

"*Além disso, a imprensa é atualmente uma forte força política que demonstra tendências partidárias e toma lados no debate político. Posto isso, também dados colhidos para fins jornalísticos devem ser submetidos à lei*". (*RubemRJ*)

Quem defende isso? *Lucas Zolet, Felipe de Ivanoff, Kaliny Aglay, andremenegazzo* e *RubemRJ*

(B) Não.

"A exclusão da atividade jornalística do escopo da lei serve ao interesse público e as liberdades de expressão e informação. Os fins jornalísticos devem, portanto, serem entendidos de forma ampla abrangendo também blogeiros e 'whistleblowers'*".*

Quem defende isso? *Joana Varon*.

4.2.6. Deve haver outras exceções para a aplicação da lei de dados pessoais? Quais?

Propostas avulsas para a regulação deste tema:

(A) Sim, a lei deveria incluir outras exceções além da finalidade jornalística.

A abertura da possibilidade de uso de dados pessoais para fins jornalísticos sem o consentimento dos titulares é uma exceção "estreita demais", deveriam ser incluídas outras exceções relacionadas ao exercício da liberdade de expressão (de cunho artístico, literário etc).

Autor da proposta: *Privacy International, Ana Amelia* e *Associação da Liberdade Religiosa e Negócios.*

Sugestões de redação:

Autor da sugestão: *Associação da Liberdade Religiosa e Negócios.*

[MODIFICAÇÃO] Art. 2º § 2º (II) realizados para fins exclusivamente jornalísticos ou para conservação de arquivos, e registros históricos, genealógicos, científicos, artísticos, acadêmicos, culturais ou estatísticos.

Autor da sugestão: *Ana Amelia.*

[MODIFICAÇÃO] Art. 2º § 2º (II) efetuados para fins exclusivamente jornalísticos ou de expressão artística ou literária, apenas na medida em que sejam necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão.

4.2.7. Como deve ser a regra geral sobre a transferência de dados pessoais de bases de dados públicas para entidades privadas?

Este parágrafo foi alvo de muitas críticas, tanto de participantes que acreditam que suas disposições são demasiadamente restritas quanto daqueles que acreditam que este tipo de transferência de dados pessoais deveria ser mais severamente controlado ou, até mesmo, proibido.

As propostas, portanto, podem ser separadas em dois grupos. O primeiro grupo **(A)** sugeriu exceções à regra geral colocada pelo parágrafo e o segundo grupo **(B)** propôs formas de melhor controlar ou coibir transferências de órgãos ou entidades públicas para entidades privadas. Criamos também um terceiro grupo **(C)**, no qual destacaremos as críticas realizadas pelo *ITI* e pelo *RELX Group*.

Propostas avulsas para a regulação deste tema:

(A) Deve haver novas exceções à regra geral de transferência de dados pessoais de bases públicas para entidades privadas.

A.1. A regra geral deve ser flexibilizada para evitar fraudes e manter segurança nos negócios.

"*É de extrema relevância que entidades privadas tenham acesso as informações cadastrais e biométricas mantidas pelos órgãos públicos de forma a verificar a autenticidade e a atualização dos dados utilizados para realização dos negócios, com o intuito principal de evitar fraudes e manter a*

segurança na concessão de crédito".

"Sugerimos incluir isenções específicas para permitir a transferência de dados pessoais para fins de bem comum, tal como emprego ou serviços de verificação de identidade, fornecimento de acesso ao crédito, gestão de riscos e prevenção contra fraudes, ameaças à segurança cibernética e outras atividades ilegais.

Sugerimos também acrescentar exceções contidas no Artigo 24 para garantir a uniformidade". (*US Business Council*)

Autor da proposta: *Boa Vista Serviços, Febraban* e *US Business Council.*

A.2. A regra geral deve ser flexibilizada quando há interesse público relevante.

"*Esse tipo de transferência deve ser admitido quando há interesse público relevante. A vedação da transferência de dados entre entidades públicas e privadas irá prejudicar o funcionamento de muitos negócios, como exemplo podemos citar o negócio das seguradoras que necessitam de, por exemplo, dados acerca dos veículos para efetuar de forma correta o pagamento de indenizações seguritárias (*sic*).*

Esse tipo de posicionamento é adotado na Europa e encontra apoio na LAI brasileira que no inciso V do §3º de seu art. 31, garante acesso a informações quando há interesse público envolvido".

Autor da proposta: *CNseg.*

(B) Devem ser criadas novas obrigações para o controle de transferências de dados de órgãos públicos para entidades privadas.

B.1. Deve ser criada a obrigação de um "termo de confidencialidade" quando uma transferência de dados de base pública para entidade privada é realizada.

"O dever de elaboração de Termo de Confidencialidade busca dar segurança jurídica à transferência de dados pessoais pela Administração Pública em casos de execução terceirizada ou concessão/permissão de atividade pública".

Autor da proposta: *Fiesp.*

(C) Demais críticas à regra geral sobre transferências de dados pessoais de órgãos públicos para entidades privadas.

C.1. A regra geral tem impacto negativo na transparência governamental.

"Este tipo de previsão legal tem impacto negativo na transparência e sobre os compromissos do Brasil de um governo aberto, tais como, por exemplo, aqueles assumidos na Parceria para Governo Aberto".

Autor da proposta: *ITI.*

C.2. É necessária uma compatibilização da regra geral com a Lei de Acesso à Informação.

"*Sugerimos alteração nesse dispositivo pois ele não está em completa harmonia com a linguagem encontrada na lei de acesso à informação do Brasil, especificamente o art. 31, II e o § 3º. Recomendam a mudança nesse dispositivo e no art. 24, I, do APL*".

Autor da proposta: *RELX Group.*

(iv) Síntese de todas as propostas nas sugestões de redação

Sugestões de redação:

Autor da sugestão: *RELX Group.*

[MODIFICAÇÃO E INCLUSÃO] Art. 2º - (...) § 3º: O tratamento de informações pessoais realizado por órgãos públicos ou entidades públicas deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como as liberdades e garantias individuais.

I - As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem podem ter sua divulgação ou acesso por terceiros autorizados por disposições legais ou consentimento expresso da pessoa a que se referem.

II - O consentimento mencionado no inciso I do parágrafo 3 não será exigido quando as informações forem necessárias para os casos constantes na Lei 12.527, de 18 de novembro de 2011, no artigo 31, parágrafo 3, incisos I, II, III, IV e V.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO E INCLUSÃO] 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:

I - quando houver consentimento, nos termos do artigo 24 desta Lei;

II- em casos de execução terceirizada;

III – para fins de obtenção, legitimação ou atualização de dados cadastrais ou biométricos por entidades privadas; ou

IV - mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] 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.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 2º - (...) 3º É vedado às entidades da Administração Pública efetuar a transferência para entidades privadas de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais, exceto em casos de concessão, autorização ou permissão de serviço público que o exija e exclusivamente para o fim específico e determinado.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] 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, devendo, neste caso, ser elaborado Termo de Confidencialidade para o fornecimento destes dados pessoais.

4.2.8. A aplicabilidade da lei em relação ao Estado deve ficar mais explícita?

Propostas avulsas para a regulação deste tema:

(A) O Estado também deve estar sujeito às determinações do APL

"Sugerimos estes novos parágrafos de forma a explicitar a obrigação do estado de cumprir com os deveres determinados pelo APL. Apesar do texto do APL explicitamente incluir as atividades do Estado em seu escopo de aplicação, ele contém exceções e especificações que merecem uma análise atenta e transversal, já que por vezes podem dar margem à relativização das obrigações do Estado e de agentes privados com relação a certos tipos de tratamento de dados pessoais".

Autor da proposta: *CTS-FGV.*

Sugestões de redação:

Autor da sugestão: *CTS-FGV.*

[MODIFICAÇÃO E INCLUSÃO] § 4º Os dados mencionados no § 3º devem ser definitivamente excluídos após o período de vigência do contrato de concessão ou permissão ou da prestação do serviço terceirizado que demandou o compartilhamento.

§ 5º As entidades privadas mencionadas no § 3º deverão comprovar a capacidade para garantir a segurança de dados a que se refere esta lei antes de sua contratação.

§ 6º Cabe ao órgão ou entidade pública comprovar a necessidade de transferência de dados pessoais para entidade privada, sob pena de responsabilização.

4.2.9. A lei deve ser aplicável a empresas públicas e sociedades de economia mista[3]?

Propostas avulsas para a regulação deste tema:

(A) A diferença de tratamento entre empresas públicas e sociedades de economia mista e empresas privadas pode causar assimetrias e problemas de concorrência

"Parágrafo Único do Art. 3º diz que as empresas públicas e de economia mista não serão tratadas como as empresas de direito privado particulares quando estiverem operacionalizando políticas públicas no tratamento de dados pessoais.".

Há um potencial risco moral nesta lacuna, porque não há como avaliar se a empresa pública ou de economia mista poderá cruzar informações recolhidas quando estiver operando uma política pública com informações de seus clientes e formar um grande banco de dados que dará a ela uma vantagem competitiva sobre as empresas privadas particulares.

*Combinando esse dispositivo com o inciso XVII do art. 5º, nota-se uma assimetria ainda maior na capacidade de competir. A empresa pública ou de economia mista poderá cruzar bancos de dados no regime "*third-party sharing opt-in*", enquanto o anteprojeto se silencia sobre direitos das empresas particulares.*

*Nesse sentido, a SEAE entende que, para essas empresas, vale o regime "*blanket opt-in*" (o regime mais restritivo e mais custoso para os fornecedores). Por isso, a SEAE entende que esta norma possui efeitos anticompetitivos* (...)*, pois desestimula a concorrência entre empresas públicas ou de economia mista e as empresas privadas particulares".*

Autor da proposta: *SEAE/MF.*

(B) Deve ser criado um dever de exclusão dos dados pessoais por parte de empresas públicas ou sociedades de economia mista após o esgotamento do tratamento dos dados ou da finalidade específica a partir da qual eles foram coletados

Autor da proposta: *ABDTIC.*

Sugestões de redação:

Autor da sugestão: *Tarso Cabral Violin.*

[MODIFICAÇÃO] Art. 3º (...) Parágrafo único. As empresas públicas e sociedades de economia mista que prestam serviços públicos, e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades de Direito Público, nos termos dessa Lei

[3] Este assunto foi realocado na nova versão do anteprojeto de lei divulgada em outubro de 2015 para o artigo 25. Inserimos o tema aqui por conta da sua presença no início do texto da versão colocada em debate público.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme reproduzido abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 2º. A disciplina da proteção de dados pessoais no Brasil tem como fundamento o respeito à privacidade, bem como:

I – a autodeterminação informativa;

II – a liberdade de expressão, comunicação e opinião;

III – a inviolabilidade da intimidade, vida privada, honra e imagem;

IV – o desenvolvimento econômico e tecnológico;

V – a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. ~~2~~3º Esta Lei aplica-se a qualquer operação de tratamento realizada por ~~meio total ou parcialmente automatizado, por~~ pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede ~~e~~ ou do país onde ~~esteja localizado o banco de~~ estejam localizados os dados, desde que:

I – a operação de tratamento seja realizada no território nacional;

II – a atividade de tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

~~II~~ III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

~~§ 1º~~ Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

~~§ 2º~~ Art. 4º Esta Lei não se aplica ao~~s~~ tratamento~~s~~ de dados:

I – realizado~~s~~ por pessoa natural para fins exclusivamente pessoais; ou

II – realizado~~s~~ para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; ou (...)

~~**Art. 3º** As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.~~

~~**Parágrafo único**. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.~~

4.3. Tratamento de dados para fins de segurança pública e do estado de defesa

REDAÇÃO LEVADA A DEBATE

Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regido por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

Surgiram muitas indagações na plataforma de consulta pública sobre a necessidade de delegar as disposições acerca dos tratamentos de dados com fins exclusivos de segurança pública, defesa e segurança do Estado a legislação específica.

Nesta questão, os participantes se dividiram, mas a grande maioria concordou que, mesmo se estes tipos de tratamento forem tratados em legislação específica, esta deverá estar em conformidade com a futura lei de proteção de dados pessoais.

4.3.1. Tratamentos de dados para fins exclusivos de segurança pública, defesa e segurança do Estado deverão ser abordados em legislação específica?

Respostas controversas coletadas na plataforma de debate:

(A) Sim, mas a discussão do tema deve ser feita em conjunto.

Para os defensores desta tese a divisão formal (em mais de uma lei) é admissível, uma vez que é possível admitir diferenças suficientes entre a proteção de dados pessoais geral e aquela relativa a tais temas. Tais atores defendem, entretanto que **é necessário discutir essa outra lei de forma simultânea com o APL já que os textos legais interagem um com o outro**.

Em outras palavras, "*separar formalmente é até admissível, mas fragmentar a discussão não é uma*

solução republicana se a iniciativa é para harmonizar os interesses conflitantes com transparência".

Quem defende isso? *Cláudio Lucena, Emerson Wendt* e *fbraga.*

(B) Não.

O texto do anteprojeto deve trazer padrões mínimos de respeito ao direito à privacidade nestas atividades empreendidas pelo Estado; ele também deve esclarecer que na ausência de lei específica a atuação do Estado deverá seguir as normas desta lei.

Quem defende isso? *ITI, GEPI-FGV, Privacy International, JCK, Margareth, Prof. Marcos, Rodrigo, Maurício Coeli* e *Marcelo Saldanha*

Também foi alvo de preocupação entre os participantes a possibilidade de um vácuo legislativo no caso de a Lei de Proteção de Dados Pessoais entrar em vigor sem que a legislação especial tenha sido ainda discutida e aprovada.

Muitos, inclusive, argumentaram que a concentração de todas as disposições na mesma lei seria a forma mais eficaz de evitar esse período de transição. O *CTS-FGV*, porém, acatando a delegação para lei específica, sugeriu disposições para regular o período de transição de forma a evitar que uma eventual demora na aprovação da lei específica fosse danosa aos direitos dos cidadãos.

Propostas avulsas para a regulação deste tema:

(A) Deve haver balizas para atuação dos órgãos de segurança pública enquanto legislação específica não é aprovada.

"Sugerimos novos parágrafos para limitar a atuação dos órgão de segurança pública enquanto não é aprovada legislação específica. Ademais, tal com aponta a experiêncua (sic) européia no âmbito dos estudos do Grupo de trabalho Article 29 (opinião 04/2014), nas hipóteses de tratamento para segurança pública, defesa e segurança do estado deverão ser observados os princípios dispostos no APL, em especial o da finalidade, da necessidade e o da proporcionalidade".

Autor da proposta: *CTS-FGV.*

Sugestões de redação:

Autor da sugestão: *CTS-FGV.*

[INCLUSÃO] §1º Até a aprovação de uma lei específica alinhada aos princípios da proteção de dados pessoais, os tratamentos previstos no caput ficam sujeitos à presente legislação.

§2º O tratamento dos dados a que se refere o caput deve ser realizado apenas sob supervisão das autoridades competentes, respeitando as proteções adequadas à garantia dos direitos fundamentais dos titulares de dados.

§3º O acesso a dados pessoais, inclusive metadados, coletados e/ou armazenados por entidades privadas por parte de autoridades públicas para fins de investigação ou repressão de infrações penais somente será autorizado mediante ordem judicial, observando os princípios estabelecidos no artigo 6º.

§4º Os dados mencionados no §4º não serão tratados de forma incompatível com as finalidades pelas quais foram originalmente obtidos, devendo ser definitivamente excluídos quando não forem mais necessários para os propósitos para os quais foram coletados.

4.3.2. A lei deve tratar de hipóteses de fornecimento de dados pessoais para autoridades?

Por fim, é necessário ressaltar as contribuições da *Fiesp* e da *Joana Varon*. A *Fiesp* buscou tratar do acesso a dados cadastrais por autoridades competentes, enquanto *Joana Varon* fez uma contribuição no sentido de balizar as disposições do artigo 4º no sentido de limitá-las a hipóteses de investigação de infrações penais mediante instauração de inquérito policial.

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever hipóteses de fornecimentos de dados cadastrais sem ordem judicial.

Sugerimos o acréscimo de dois novos parágrafos. O anteprojeto representa uma boa oportunidade para por fim a dúvida quanto a possibilidade de autoridades requererem dados cadastrais sem a necessidade de ordem judicial para fins de investigação criminal.

Autor da proposta: *Fiesp.*

(B) Esta exceção de aplicabilidade deve limitar-se a investigações de infrações penais

"Este dispostivo (sic) deve se limitar a tratar unicamente e exclusivamente de investigação de infrações penais mediante instauração de inquérito policial, nos termos do Código de Processo Penal, seguindo os principios da necessidade e proporcionalidade. Somente dessa forma, a presunção de inocência pravelece (sic) e evita-se a abertura legal para a vigilância massiva por parte do estado".

Autora da proposta: *Joana Varon.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[INCLUSÃO] § 2º Autoridades administrativas ou o Ministério Público, que detenham competência legal para a sua requisição, poderão ter acesso, independentemente de ordem judicial, aos dados cadastrais que informem qualificação pessoal, filiação e endereço, mantidos pelo responsável, operador ou encarregado pelos dados.

§ 3º Exceto disposição em Lei específica ou prevista nesta Lei, a disponibilização de todos os demais dados ou conteúdo de comunicações privadas pelo responsável, operador ou encarregado dos dados, dependerá de ordem judicial.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 4º**~~ **III** ~~– Os tratamentos de dados pessoais~~ realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais~~, serão regidos~~.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~**Parágrafo único.**~~ **§ 2º** É vedado o tratamento dos dados a que se refere o ~~caput~~ inciso III por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

§ 3º O órgão competente emitirá opiniões técnicas ou recomendações referentes às exceções previstas nos incisos II e III, bem como poderá solicitar aos responsáveis relatórios de impacto à privacidade.

4.4. Definições

REDAÇÃO LEVADA A DEBATE

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

II – tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;

IV – dados anônimos: dados relativos 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 para identificar o referido titular;

V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;

VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;

VII – consentimento[4]: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;

X – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;

XI – interconexão: transferência de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;

XII – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma;

XIII – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;

[4] Os comentários desse dispositivo foram deslocados para a discussão travada no artigo 7 que trata, especificamente, sobre o consentimento.

XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;

XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e

XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

4.4.1. O conceito de dados pessoais deve ser restringido ou alargado[5]?

O conceito de dados pessoais é um conceito chave, pois é o que delimitará o escopo de aplicação da lei. Nesse sentido, as participações rivalizaram-se entre defender a sua restrição ou sua ampliação.

Respostas controversas coletadas na plataforma de debate:

(A) Deve ser restringido para...

A.1. ... alcançar, apenas, um sujeito identificável em nível individual (*Câmara BR*);

A.2. ... excluir de sua definição os dados cadastrais (*Boa Vista Serviços*);

> Os dados cadastrais – nome, endereço físico e eletrônico, telefone, RG ou CPF/CNPJ, sexo, profissão, filiação, naturalidade, nascimento, estado civil e óbito – são elementos relacionais públicos, individualizando de maneira objetiva o cidadão. Desta forma, eles deveriam conter uma diferenciação conceitual para resguardar o interesse da coletividade na identificação dos indivíduos.

A.3. ... valer apenas quando o responsável pelo tratamento tiver interesse em identificar a pessoa em causa (*Cisco* e *BSA*);

> Seria desproporcional exigir medidas de proteção, quando o responsável pelo tratamento dos dados não está realmente tentando identificar o seu titular (*Cisco*). Nesse sentido, deveria ser

[5] O debate em torno dos dados anônimos também está no cerne dessa discussão, mas foi reportado em tópico próprio pela densidade da discussão e pluralidade de argumentos.

adotado um conceito de dados pessoais "baseada no contexto", sob o qual os dados devam ser considerados como pessoais somente quando o responsável pelo tratamento tiver condições efetivas para identificar o seu titular. Isto porque, o contexto e as circunstâncias particulares de um caso específico têm um impacto direto sobre tal possibilidade de identificação (Parecer 05/2014 do European Advisory Board Working Party 29). (*BSA*).

A.4. ... que a expressão "identificável" esteja acompanhada de termos como "facilmente", "prontamente" ou "razoavelmente" (*MPA, ITI, US Business Council, IAB, RELX Group, ABRANET* e *Maria Cunha e Melo*[6]);

O conceito de dados pessoais seria extremamente abrangente, alcançando, praticamente, todos os dados existentes que sempre guardariam essa potencialidade de identificar alguém. Com relação ao termo "razoavelmente", um dos defensores dessa tese atenta que essa sugestão encontra inspiração na legislação canadense e no âmbito da regulação geral de proteção de dados da Europa (*Iab*).

A.5. ... excluir números identificativos, dados locacionais ou identificadores eletrônicos (*Febraban, ESA, BSA*).

A delimitação de dados pessoais deve se pautar por uma clara e inequívoca identificação do titular para fins de estabelecer direitos e obrigações (*Febraban*). Esses tipos de dados (endereços de IP, identificadores de cookies, etc.) não necessariamente permitem a identificação de indivíduos, mas somente a identificação de computadores ou terminais. A adoção de um conceito mais abrangente de dado pessoal (como o atualmente proposto) pode desincentivar a condução de negócios que necessitem tais tipos de dados (*ESA*). É provável que a aplicação de obrigações jurídicas muito rigorosas aplicada a uma vasta gama de dados reduza a inovação no Brasil, havendo um impacto negativo sobre o crescimento econômico. Por exemplo, dados de localização que não estejam ligados a uma pessoa identificável (tais como o nome de uma rede sem fio local) levantam menos questões de privacidade e não merecem ser regulamentados como dados pessoais. (*BSA*)

Quem defende isso? *Câmara BR, Boa Vista Serviços, Cisco, BSA, MPA, ITI, US Business Council, IAB, RELX Group, ABRANET, Maria Cunha e Melo, Febraban* e *ESA.*

(B) Deve ser alargado para...

B.1. ... abranger a possibilidade de identificação do indivíduo ocorrer forma direta ou indireta (*CTS-FGV, Privacy Information, Marcos Baldin e MVianna, Ana Amelia, Katia Cavalcanti, Wellington Cremasco e Gabriele Ferreira*);

Fortalecer-se-á a esfera de proteção do indivíduo (*CTS-FGV*), já que qualquer informação pode ser usada para identificar um indivíduo, ainda que não diretamente a ele relacionada. Esse seria o caso, por exemplo, do *profiling* e de mecanismos de rastreamento (*tracking*) que independem de um endereço, um nome específico ou outros identificadores diretos para afetar um sujeito em específico (*Privacy International*). Ou mesmo dados bancários e financeiros, de rendimentos e padrões de comportamento que poderia também, indiretamente, identificar um indivíduo (*Marcos Baldin* e *MVianna*). Alguns defensores dessa tese sustentam que tais termos – direta e indiretamente – nortearam e delimitariam o alcance

[6] Os defensores dessa tese procuram vincular o conceito de dados pessoais ao de dados anônimos. Ambos os conceitos deveriam ser orientados pelo termo razoavelmente/razoável. Assim, uma vez que dados anônimos seriam aqueles que não são "suscetíveis de serem razoavelmente utilizados para identificar" um indivíduo, eles estariam fora do escopo da lei por conta dessa nova definição de dados pessoais sugerida, qual seja, um dado que identifique ou permita por meios razoáveis a efetiva identificação da pessoa natural. Essa coincidência de termos "razoável/razoavelmente" criaria, portanto, uma conceituação mutualmente excludente entre dados pessoais e dados anônimos para delimitar o âmbito de aplicação da lei.

da palavra identificável, torando, assim, mais clara a redação do conceito de dados pessoais (*Ana Amelia, Katia Cavalcanti, Wellington Cremasco* e *Gabriele Ferreira*).

B.2. ... que os números identificativos, dados locacionais ou identificadores eletrônicos estejam, necessariamente, associados a um determinando período de tempo (*SindiTeleBrasil*);

Em vista de que há IPs fixos e dinâmicos e, no caso dos dinâmicos, o número de identificação deve estar relacionado a um determinado período de tempo para identificar um indivíduo, deveria haver a inclusão de tal elemento temporal para se assegurar o conceito de dado pessoal.

B.3. ... acrescer quaisquer tipos de informações, isoladas ou agregadas, que possam sujeitar um indivíduo a um tratamento total ou parcialmente automatizado (*GPoPAI*);

Deve-se expandir o conceito de dados pessoais para incluir parâmetros tecnologicamente neutros e abertos. Não se deveria limitar o conceito de dados pessoais ao de identificadores eletrônicos, o que pode se tornar obsoleto ao longo tempo. Por isso, a importância em alargar o conceito de dados pessoais para cobrir toda e qualquer informação, isolada ou agregada, que sujeite um determinado indivíduo a um processo de decisão automatizada.

B.4. ... incluir a possibilidade de identificação por som e imagem (*Margareth* e *Amanda HN*).

Quem defende isso? *CTS-FGV, Privacy International, Marcos Baldin e MVianna, Ana Amelia, Katia Cavalcanti, Wellington Cremasco, Gabriele Ferreira, SindiTeleBrasil, GPoPAI*, *Margareth* e *Amanda HN.*

Sugestões de redação:

Autor da sugestão: *CTS-FGV.*

[MODIFICAÇÃO] I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, direta ou indiretamente, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] I – dado pessoal: qualquer informação relativa a uma pessoa natural identificada ou identificável, com exceção de dados tornados anônimos por meios técnicos e de dados que apenas identificam o terminal ou aparelho e não uma pessoa natural; é considerado identificável todo aquele que possa ser facilmente ou prontamente identificado, através dos dados coletados;

Autor da sugestão: *Febraban e ESA.*

[MODIFICAÇÃO] I – dado pessoal: quaisquer dados relacionados à pessoa natural que a torne identificada ou identificável, de forma inequívoca;

Autor da sugestão: *IAB.*

[MODIFICAÇÃO] I – dado pessoal: dado que identifique ou permita, por meios razoáveis, a efetiva identificação da pessoa natural;

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável no nível individual, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos, desde que tais permitam a identificação, através de formas razoáveis, da pessoa natural pelo responsável pelo tratamento de dados pessoais;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO E INCLUSÃO] I – dados pessoais: dados relacionados à pessoa natural identificada ou razoavelmente identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos.

a) os dados pessoais não incluirão: dados não identificáveis ou anônimos.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos associados a um determinado momento no tempo.

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] I – (...) ou identificadores eletrônicos, incluindo informações, isoladas ou agregadas, que possam sujeitar um indivíduo a um tratamento total ou parcialmente automatizado;

Autor da sugestão: *Ana Amelia, Katia Cavalcanti, Wellington Cremasco e Gabriele Ferreira.*

[MODIFICAÇÃO] I – dado pessoal: qualquer informação relacionada à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos; é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social;

Autor da sugestão: *BSA.*

[MODIFICAÇÃO] I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável;

Autor da sugestão: *RELX Group.*

[MODIFICAÇÃO] I - dado pessoal: dado relacionado à pessoa natural identificada ou

razoavelmente identificável, inclusive (...);

4.4.2. A conceituação da atividade de tratamento de dados pessoais é problemática?

Para definir o que é tratamento de dados pessoais, utilizou-se da técnica legislativa de listar uma série de ações que cairiam dentro de tal conceituação. Ao todo foram utilizados 24 (vinte e quatro) substantivos para descrever a atividade de tratamento de dados pessoais. Dessa definição extensa, sobrevieram contribuições que apontaram algumas falhas dessa conceituação, propondo a exclusão/revisão de alguns dos termos enumerados.

Propostas avulsas para a regulação deste tema:

(A) O termo "recepção" deve ser excluído.

Recepção de forma isolada de dados pessoais não deve ser considerada como hipótese de tratamento de dados, já que não representa uma capacidade efetiva de utilização dos dados [*ABRANET*].

Autores da Proposta: *Câmara BR* e *ABRANET.*

(B) O termo "transporte" deve ser excluído.

O termo "transporte" tem o mesmo significado de transmissão, de modo que seria inútil tal sobreposição. Além do mais, a palavra transporte pode abranger, indevidamente, transporte físico, e, assim, gerar consequências tributárias a acarretar um ônus tanto para as indústrias, como para os titulares dos dados [*Câmara BR* e *ABRANET*].

Autores da Proposta: *Câmara BR*, *Cisco, ITI* e *ABRANET.*

(C) O termo "interconexão" deve ser excluído ou substituído.

O termo "interconexão" poderia ter como sinônimo a palavra transmissão. Além do mais, "interconexão" pode ter consequências tributárias por ser tipicamente utilizado com outras características em telecomunicações (incide ICMS sobre interconexão em telecomunicações) [*ABRANET*]. Um dos defensores dessa tese sugere a sua substituição pelo termo cruzamento [*ABDTIC*].

Autores da Proposta: *Câmara BR*, *ABRANET* e *ABDTIC*.

(D) Os termos "transmissão", "recepção", "distribuição" e "transporte" devem ser excluídos em bloco.

Haveria uma confusão de análise com ações que visam a divulgação e fornecimento dos dados a terceiros. É o caso, por exemplo, da transmissão, recepção, distribuição e transporte. Tais ações têm como finalidade o transporte de dados de um lugar para outro, sem caracterizar, portanto, a

atividade de tratamento.

Autor da proposta: *SindiTeleBrasil.*

(E) O termo "coleta" deve ser excluído.

A coleta de dados não se confunde com a atividade de tratamento. Tratam-se de noções distintas, já que o próprio artigo 2º do APL estabeleceria, contraditoriamente, tal diferenciação, trazendo uma outra conceituação.

Autor da proposta: *SindiTeleBrasil.*

(F) O conceito de "tratamento" deve abranger qualquer tratamento de dados – não somente o tratamento de dados pessoais.

O conceito deve abarcar aquilo que vem a ser o tratamento de dados no geral e não de dados pessoais, já que existe tratamento de dados que não são, necessariamente, considerados pessoais de acordo com a própria definição contida no artigo 5º, I.

Autor da proposta: *SindiTeleBrasil.*

(G) Os termos "bloqueio" e "fornecimento de dados pessoais a terceiro" devem ser excluídos.

As ações de bloqueio ou fornecimento a terceiros de dados pessoais deveriam ser limitadas pela legislação e, portanto, não deveriam ser legitimadas por dessa definição geral de tratamento de dados pessoais.

Autor da proposta: *JCK*.

(H) Os termos "arquivamento" e "transmissão" devem ser excluídos.

Os termos "transmissão" e "arquivamento" encontrariam seus sinônimos, respectivamente, em distribuição e armazenamento, dispensando, por isso, a sua enumeração nessa conceituação.

Autor da proposta: *ABDTIC*.

(H) Os termos "descaracterização", "anonimização" e "encriptação" deve ser excluídos da definição do que é tratamento de dados pessoais.

A exclusão das atividades de descaracterização, anonimização e encriptação são medidas favoráveis à privacidade. Assim sendo, elas deveria estar fora dessa conceituação, a fim de fomentar a sua adoção pelas empresas para uma melhor proteção dos pessoais dos brasileiros.

Autor da proposta: *ITI*.

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] II - tratamento: toda ação ou conjunto de ações de classificação, modificação, produção, comparação, avaliação, controle, organização, seleção, extração, utilização, bloqueio e cancelamento de dados para fins de análise, bem como o seu fornecimento ou a sua divulgação a terceiros por comunicação, interconexão, transferência, difusão ou extração;

Autor da sugestão: *JCK.*

[MODIFICAÇÃO] II – tratamento: conjunto de ações, operações e funções referentes a coleta, inserção, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, por comunicação, interconexão, transferência, difusão ou extração;

4.4.3. Deve haver uma diferenciação entre dados pessoais e dados sensíveis?

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

Deve haver divisão entre tipos de dados para garantir a alguns uma proteção extra. A separação dos "dados sensíveis" já existe há muito tempo (e.g., A Diretiva da União Europeia datada de 1995). Ela se deve ao seu maior potencial lesivo desses dados que está, intimamente, relacionada à proteção de direitos fundamentais: como a não descriminação [*Margareth*]. Por isso, um tratamento desigual aos dados sensíveis é uma medida de equilíbrio na exata medida do seu maior potencial lesivo [*Giovanna*].

Quem defendeu isso? *Margareth* e *Giovanna Carloni* (e os demais participantes dessa discussão, que ao discutir sobre a ampliação ou restrição do conceito de dados sensíveis, concordam, implicitamente, com essa diferenciação).

(B) Não.

Não deveria haver divisão entre tipos de dados. Todos os dados deveriam ter o mesmo tratamento e o mesmo grau de proteção. A classificação de dados por sua sensibilidade apenas abre espaço para que alguns tipos de dados não sejam tão protegidos quanto outros.

Quem defendeu isso? *JCK.*

4.4.4. O conceito de dados sensíveis deve ser restringido ou alargado?

Os dados sensíveis foram conceituados de maneira exemplificativa. Isto é, por meio de uma lista foram enumerados quais dados seriam considerados sensíveis. Nesse contexto, as contribuições rivalizaram-se no sentido de alargar ou restringir essa conceituação.

Respostas controversas coletadas na plataforma de debate:

(A) Restringido para...

A.1. ... exclusão das palavras filosóficas ou morais (*Câmara BR, ITI, US Business Council* e *ABDTIC*);

> Tais termos seriam subjetivos e vagos. Isso poderia ocasionar margem para interpretações muito ampliativas e equivocadas de dados sensíveis Nesse sentido, um dos defensores dessa tese argumenta que deveria ser substituído o verbo "revelem" pelo termo "dados consistentes em" para uma melhor delimitação daquilo o que viria a ser considerado como dado sensível: somente aqueles que representassem, diretamente, os exemplos listados para tal conceituação [*ABDTIC*].

A.2. ... melhor delimitação dos dados referentes à saúde (*ITI* e *US Business Council*).

> Dados de saúde podem incluir uma vasta quantidade de informações que não devem ser caracterizadas como sensíveis. Por exemplo, a frequências cardíaca de uma pessoa que é registrada por um aplicativo de corrida. Diferentemente, o estado de saúde de uma pessoa, por meio de seus registros médicos, deve ser considerado como um dado sensível.

Quem defende isso? *Câmara BR, ITI, US Business Council* e *ABDTIC.*

(B) Ampliado para...

B.1. ... abranger dados biométricos (*GPoPAI, Fiesp, Marcos Baldin, Stefan, Wellington Cremasco, Proteste, Margareth* e *Ana Amelia*);

> Os dados biométricos seriam identificadores únicos em razão do seu grau de precisão. Dada a característica imutável do corpo de uma pessoa, eles seriam mais singulares até que outros tipos de dados pessoais usados para a identificação de uma pessoa. Por exemplo, os registros de identidade e o número no cadastro nacional de pessoas físicas. Por tal razão, eles deteriam um potencial lesivo elevado, pois, a partir deles, seu titular estaria exposto aos mais variados tipos de fraudes e roubos de identidade [*GPoPAI*]. Além do mais, o próprio texto do APL ressalva a possibilidade deles serem considerados como tal (artigo 13, §2°), o que determinaria a sua inclusão na definição (lista) de dados sensíveis por uma questão de coerência [*Fiesp*].

B.2. ... abranger dados financeiros e/ou condições socioeconômicas (*GPoPAI, Marcos Baldin, Stefan, Wellington Cremasco, Proteste, Margareth* e *Ana Amelia*);

> Na medida em que a criação da categoria de dados sensíveis justifica-se por ser um tipo de informação que pode ocasionar práticas discriminatórias, ela deve, então, abranger dados que revelem a classe social e a capacidade econômica de uma pessoa que podem resultar no mesmo efeito discriminatório. Os defensores dessa tese divergem, apenas, quanto à terminologia: a) socioeconômica [*GPoPAI, Proteste*]; b) dados financeiros [*Marcos Baldin, Stefan, Wellington Cremasco, Proteste* e *Margareth*]; c) econômica [*Ana Amelia*]

B.3. ... abranger dados sobre identidade física, fisiológica e psíquica (*Ana Amelia*);

Quem defende isso? *GPoPAI, Fiesp, Marcos Baldin, Stefan, Wellington Cremasco, Proteste, Margareth* e *Ana Amelia.*

Sugestões de redação:

Autor da sugestão: *Proteste.*

[MODIFICAÇÃO] III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a 4 sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, às condições socioeconômicas, bem como dados genéticos e dados biométricos, observando-se quanto a esse último o disposto no artigo 13, §2°;

Autor da sugestão: *Ana Amelia.*

[MODIFICAÇÃO] III – dados sensíveis: dados pessoais identificáveis que revelem, direta ou indiretamente, a um ou mais elementos específicos de sua identidade física, fisiológica, psíquica, econômica, cultural ou social, a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes às condições de saúde ou à vida sexual, bem como dados genéticos expressamente relacionados a um registro médico ou individual;

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos e biométricos;

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] III – dados sensíveis: (...) dados referentes à saúde ou à vida sexual, às condições socieconômicas, bem como dados genéticos e dados biométricos, observando-se quanto a esse último o disposto no art, 13, § 2º.

4.4.5. Dados anônimos devem ser considerados dados pessoais?

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

"Adicionar dados anônimos como novo inciso é inconcebível. Dados anônimos também são dados pessoais e, portanto, dentro do escopo da lei, inclusive porque a "autoridade de proteção de dados" deve fiscalizar técnicas de anonimização de acordo com o estado da arte e padrão tecnológico, ou seja, aquele que não seguir a forma correta de anonimização será responsabilizado".

Quem defende isso? *Joana Varon.*

(B) Não.

Segundo os defensores desta tese "*a utilização da anonimização dos dados permite que se utilize dados para tomadas de decisões e se alcancem resultados sem que haja qualquer tipo de identificação das pessoas envolvidas*". Nesse sentido, dados anônimos não devem ser considerados dados pessoais e, portanto, não devem estar no escopo da lei.

Quem defende isso? *ABRANET, Claro, IAB, CNseg, Câmara BR* e *Vivo*.

4.4.5. Dados anônimos devem estar dentro do escopo de aplicação da lei?

Talvez essa tenha sido uma das discussões mais polarizadas do debate público. Houve um intenso embate entre quem sustentava que dados anônimos devem estar dentro do escopo da lei, e que, portanto, deveriam ser enquadrados no conceito de dados pessoais e quem, por outro lado, afirmava ser necessária a total exclusão dos dados anônimos do âmbito de aplicação da lei.

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

O processo de anonimização dos dados pessoais é, sempre, um processo reversível. Com a tecnologia do *Big Data* associada à prática de agregação de dados tem se tornado, totalmente, falaciosa essa figura dos dados anônimos [*Bruno R. Bioni*]. Haverá sempre um risco de reindetificação, o que torna o dado anônimo algo, totalmente, elusivo. Em razão dessa potencialidade inerente do dado anonimizado levar à identificação de um indivíduo, é a razão pela qual ele deve estar dentro do escopo da lei [*Maria Cunha de Melo, GPoPAI, Joana Varon, Veridiana/Intervozes*].

Uma parcela significativa dos defensores propõe, inclusive, a substituição do termo dados anônimos por dados anonimizados. Procura-se enfatizar o processo de anonimização, ao invés de se criar uma qualificação (anônimo) que não guardaria correspondência com a realidade, sendo, apenas, uma ficção [*GPoPAI, CTS-FGV, Veridiana/Intervozes, Joana Varon*]

Quem defendeu isso? *Inês Barros do Nascimento, Joana Varon, Proteste, Bruno R. Bioni, Maria Cunha de Melo, Veridiana/Intervozes, GPoPAI, CTS-FGV.*

(B) Não.

Dados anônimos não devem ser considerados como dados pessoais, já que a técnica de anonimização é uma forma "eficaz" para quebrar o vínculo entre um dado e um indivíduo. Mesmo que hajam riscos de reversão desse processo, esse risco é "insignificante" [*RELX Group*]. Isso é, justamente, o que o próprio APL visa estabelecer ao conceituar dado anônimo como aquele que não é suscetível de ser, razoavelmente, utilizado para identificar um indivíduo [*Cisco*]. Por isso, o tratamento de dados anônimos deve ser feito sem quaisquer exigências e formalidades [*Brasscom*].

Quem defendeu isso[7]? *MPA, ITI, US Business Council, RELX Group, IAB, Brasscom, Cisco, Centre for Information Policy Leadership.*

Propostas avulsas para a regulação deste tema:

(A) Os dados anônimos devem estar dentro do escopo da lei, mas com um regime jurídico mais flexível em comparação aos dados pessoais.

A.1. O regime para dados anônimos deve se caracterizar pela desnecessidade de consentimento do titular (*Bruno R. Bioni Maria Cunha de Melo*, *Claro, Câmara BR, Veridiana/Intervozes, CTS-FGV, Joana Varon, GPoPAI[8]*).

> A anonimização dos dados pessoais é, em primeiro lugar, um padrão de segurança favorável à proteção da privacidade dos usuários e, que, portanto, deve ser encorajado [*GPoPAI, Bruno R. Bioni, Maria Cunha de Melo, CTS-FGV*]. Em segundo lugar, porque existem uma série de inovações – seja no sentido de formulações de políticas públicas (cidades inteligentes), seja no âmbito de novos modelos de negócio – que são dependentes da mineração de base de dados volumosas e, que, portanto, seria inviável colher o consentimento de todos os titulares dos dados pessoais (*Bruno R. Bioni*). Por isso, a proposta de descolar os dados anônimos como uma das exceções do consentimento, sem prejuízo de todas as demais disposições legais – como, por exemplo, os princípios da adequação, necessidade não discriminação [*Veridiana/Intervozes, Joana Varon, Bruno. R. Bioni*] – seria a mais equilibrada para congregar a proteção dos dados pessoais e o próprio desenvolvimento socioeconômico dependente da mineração dos dados pessoais.

A.2. O regime para dados anônimos deve ser flexibilizado para não conferir ao titular um direito de acesso a seus dados (*ITS-Rio*).

> Seguindo essa nova racionalidade regulatória proposta, os titulares dos dados pessoais anonimizados não deveriam ter o direito de acesso a eles. Até mesmo porque, isso demandaria, em última análise, a reversão do processo de anonimização.

---

7 Uma parcela desses participantes (*Bruno R. Bioni, Maria Cunha de Melo, Veridiana/Intervozes, GPoPAI, CTS-FGV*) defende que os dados anônimos devem estar dentro do escopo da lei, mas com a sugestão de um regime jurídico mais flexível em comparação aos dados pessoais. Esse tema será retomado como uma proposta avulsa para regular dados anônimos.

8 A participante Maria Cunha de Melo não fala especificamente do consentimento, a participante fala em uma parcela da proteção legal para dados anônimos. O GPoPAI, por sua vez, propõe um teste para limitar tal exceção. Há também a preocupação de que essa hipótese poderia esvaziar a regra de que o titular deve consentir para o fluxo de seus dados pessoais. Tal discussão será retomada no artigo 11 por se confundir com a nova hipótese de interesses legítimos.

4.4.6. Quais devem ser as obrigações legais para prevenção e segurança com relação à eventuais incidentes de reidentificação de base de dados anonimizadas?

Uma vez asseverada a premissa de que os dados anonimizados podem ser reidentificados, houve uma série de contribuições para regular eventuais incidentes, seja para preveni-los, seja para trazer segurança ao próprio processo de anonimização e a seus respectivos responsáveis. Tais contribuições não se rivalizam entre si, pois a escolha de uma delas não inviabiliza o acolhimento das demais.

Propostas avulsas para a regulação deste tema:

(A) Proibição legal de reversão do processo de anonimização.

A proibição da reversão do processo de anonimização é para, justamente, proteger a privacidade, a fim de se coibir abusos com a re-identificação de um indivíduo [*Luiz Perin Filho*]. Além do mais, isso essa seria uma consequência lógica para que não seja distorcida a exigência do consentimento, que é a regra geral para o tratamento de dados pessoais [*GPoPAI*]

Autores da proposta: *GPoPAI, Veridiana/Intervozes, ABDTIC e Luiz Perin Filho.*

(B) Dever de elaboração de relatórios de transparência e impacto à privacidade e de autorização do órgão competente.

O problema da reversão do processo de anonimização está atrelado, prioritariamente, com a possibilidade se agregar base de dados diferentes para serem estabelecidas correlações, a fim de se identificar um indivíduo. É o que se chama de entropia da informação. Por isso, não basta, tão somente, proibir a desanonimização, mas, sobretudo, criar mecanismos que tragam transparência ao fluxo de base de dados anonimizadas, mediante, inclusive, uma análise do impacto que o compartilhamento de tais bases de dados poder gerar para a privacidade (a reversão do processo de anonimização). No âmbito do setor público, deveria haver, ainda, a autorização do órgão competente para se evitar abusos, mitigando-se tais riscos de re-identificação.

Autores da proposta: *GPoPAI.*

(C) Dever de autorização do órgão competente para a disponibilização pública parcial ou total de uma base de dados anonimizada.

Diversas pesquisas em que se comprovou a falácia teórica dos dados anônimos ocorreram devido a disponibilização ao público da base de dados anonimizadas. Foi, com essa oportunidade, que pesquisadores reverteram o processo de anonimização (Caso AOL e Netflix, por exemplo). Logo, o órgão competente deve avaliar tais riscos, exercendo um controle prévio (autorização) para tais hipóteses.

Autores da proposta: *GPoPAI.*

4.4.7. Qual deve ser o critério adotado para permissão de procedimentos de anonimização?

Propostas avulsas para a regulação deste tema:

(A) O órgão competente deve definir *a posteriori*.

Na incerteza do que seja razoável, se: a) os procedimentos que o mercado emprega para desanonimizar dados ou b) o estado atual da arte da tecnologia para re-identificar dados anônimos, sugere-se que essa definição seja delegada ao "órgão competente" que, a posteriori, explicitaria esse conceito vago.

Autores da proposta: *Bruno R. Bioni.*

(B) O conjunto de meios suscetíveis razoáveis para a identificação deve ser restrito àqueles que podem ser imputados ao responsável pelo tratamento de dados pessoais.

Não se deve levar em conta as possibilidades e variações que qualquer outra pessoa poderia empregar para reindetificar um dado anonimizado. Isto alargaria, demasiadamente, esse risco, na medida em que o responsável desconhece as outras técnicas que podem ser utilizadas por terceiros para tanto [*Brasscom*].

Autores da proposta: *IAB, Câmara BR* e *Brasscom.*

(C) O critério deve levar em conta a relação entre tempo, custo e mão de obra.

A relação, tempo, custo e mão de obra deve determinar o que venha a ser um meio suscetível razoável para a identificação de um sujeito. Somente, assim, haverá um critério proporcional para tornar clara a aplicação dessa regra.

Autor da proposta: *CNseg.*

(D) O critério deve levar em conta a finalidade do tratamento dos dados e a probabilidade de reidentificação.

A discussão em torno da anonimização dos dados deveria levar em conta a finalidade do tratamento de dados em curso e dos mecanismos utilizados para impedir/dificultar a identificação dos titulares dos dados (por exemplo, o uso de criptografia). Ou seja, não se trata simplesmente da mera possibilidade de re-identificação do titular do dado, mas sim de uma probabilidade real a ser aferida de acordo com a finalidade do tratamento dos dados e dos mecanismos utilizados para dificultar essa identificação.

Autor da proposta: *ITS-Rio.*

Sugestões de redação:

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] IV – dados anônimos: dados relativos a um titular, mas a partir dos quais a identidade do titular não possa ser razoavelmente identificados, nem pelo responsável pelo tratamento nem por qualquer outra pessoa com acesso ao conjunto de dados, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] IV – dados anônimos: dados sobre um titular que não possa ser identificado, pelo responsável pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;

Autor da sugestão: *Inês Barros do Nascimento.*

[MODIFICAÇÃO] IV – dados anônimos: dados pessoais relativos 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 para identificar o referido titular;

Autor da sugestão: *Proteste.*

[INCLUSÃO] [novo inciso] – dados reidentificados: são dados pessoais em razão da possível reversibilidade do processo de anonimização;

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] [novo inciso] – anonimização: ato de tornar um dado não correlacionável ao seu titular, utilizando-se de técnicas que procurem não identificá-lo, direta ou indiretamente, com um indivíduo. Os dados anônimos são, para fins desta lei, dados pessoais em razão da reversibilidade de seu processo, ainda que disponha de regras próprias nos termas desta legislação;

4.4.8. Qual deve ser a definição de "bancos de dados" na lei?

Propostas avulsas para a regulação deste tema:

(A) O conceito de banco de dados deve ser ampliado para alcançar bancos de dados não estruturados.

A definição deve ser ampliada, pois um banco de dados pode não ser, necessariamente, estruturado. Assim, estariam abrangidos não só bancos de dados relacionais tradicionais, mas, também, novas formas de bancos de dados, como grafos e *document-based*, além de arquivos simples.

Autores da proposta: *JCK, Margareth* e *ITI* (muito embora esse último, traga, apenas, a reflexão se seria mesma a intenção da lei excluir banco de dados não estruturados).

(B) A definição deve ser refinada para agregar o adjetivo "pessoais".

Para limitar a aplicação lei a dados pessoais, tornando-se coerente a definição de banco de dados. Isto porque, existem uma série de bancos de dados que não são compostos por informações pessoais.

Autores da proposta: *Gabriela Martins* e *Giovana Carloni.*

Sugestões de redação:

Autor da sugestão: *JCK* e *Margareth.*

[MODIFICAÇÃO] V - banco de dados: toda forma de armazenamento de dados pessoais, estruturado ou não, organizado ou não, localizado em um ou mais locais, física ou eletronicamente;

4.4.9. As pessoas jurídicas deveriam ser também consideradas como titulares de dados pessoais?

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

A pessoa jurídica deve ser protegida pela lei, pois a utilização indevida dos seus dados pode causar um prejuízo até maior com relação a uma pessoa natural. Esse é o caso, por exemplo, de informações sigilosas da empresa.

Quem defendeu isso? *Flavio Costa*.

(B) Não.

A lei destina-se à proteção de pessoas naturais. As pessoas jurídicas possuem outras formas de proteção de seus dados (contratos, confidencialidade, concorrência desleal, etc.). Eventualmente, no caso de inclusão das pessoas jurídicas, haveria a necessidade de se criar um capítulo próprio e específico, diferenciando-se essa técnica/dinâmica de proteção

Quem defendeu isso? *Giovanna Carloni.*

4.4.10. Com relação à definição de "titular", deve haver direito de herança aplicável a dados pessoais?

Propostas avulsas para a regulação deste tema:

(A) Deve haver direito de herança sobre dados pessoais.

A noção de titularidade de dados pessoais deve levar em consideração os direitos de sucessão. Os sucessores devem ter direito de herança sobre os dados pessoais – uma espécie de direito de propriedade sobre eles. O ideal seria admitir, após alguns meses do falecimento, que bastaria, por exemplo, a manifestação de qualquer sucessor para proibir a divulgação de dados. A discussão seria se essa proibição deveria partir de uma ação afirmativa (*opt-in*) ou se ela seria presumida (*opt-out*) pelo silêncio dos sucessores.

Autores da proposta: *Roberto Taufick*.

4.4.11. Qual deve ser a definição de "responsável" pelo tratamento de dados pessoais na lei?

Propostas avulsas para a regulação deste tema:

(A) Deve-se se separar com clareza os papéis do responsável e do operador.

Segundo os participantes que advogaram por tal posição a redação do anteprojeto de lei levada à debate não define ou identifica com clareza o responsável.

Autores da proposta: *SindiTeleBrasil* e *JCK*.

Sugestões de redação:

Autores da sugestão: *JCK* e *SindiTeleBrasil*

[MODIFICAÇÃO] VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem compete a guarda, proteção e preservação de tais dados pessoais em razão de sua posse para tratamento, administração ou arquivamento;

4.4.12. Definições legais de "comunicação de dados", "interconexão", "difusão" e "transferência"

Propostas avulsas para a regulação deste tema:

(A) A lei não deve trazer diferenciação entre as definições de "comunicação de dados", "interconexão", "difusão" e "transferência".

"Sugere-se a fusão dos termos 'comunicação de dados', 'interconexão', 'difusão' e 'transferência', preferencialmente ampliando a definição de "transferência" para abranger todas as definições" [*ABRANET*].

Autores da proposta: *ABRANET* e *Câmara BR*.

(B) As definições de "interconexão" e "difusão" devem ser suprimidas[9].

"Sugerimos a exclusão do inciso [sobre "interconexão"] *que traz uma nova definição para um termo já de corrente uso no contexto de telecomunicações e pode, portanto, causar confusão.*

Interconexão é uma expressão específica, com definição contida em legislação específica (Lei no. 9.472/97), constituindo-se na ligação entre redes de telecomunicações funcionalmente compatíveis para viabilizar um serviço de telecomunicações, com todas as implicações legais e tributárias que tal qualificação implica".

"Sugerimos a exclusão da definição [de "difusão"]*, para evitar a utilização de palavra que possuam caráter de sinônimo, para uma melhor técnica legislativa".*

Autor da proposta: *Brasscom.*

(C) A definição de "interconexão" é ampla e pode gerar confusão com a de "comunicação de dados".

"Sugerimos nova redação devido ao fato de que a redação atual é muito ampla e não deixa clara a diferença entre comunicação e interconexão de dados. O conceito de interconexão se refere ao cruzamento entre duas bases ou ficheiros de dados diferentes".

Autor da proposta: *Vivo.*

(D) A definição de "interconexão" deve trazer uma ressalva quanto à transferência de dados anônimos.

"Sugere-se que a definição de interconexão faça uma ressalva quanto à transferência de dados anônimos. A ABEP adota a posição de que dados agregados e anonimizados não devem ser considerados dados pessoais para os fins da lei.

Para a ABEP, isso seria essencial para que o Brasil possa participar dos benefícios do 'Big Data', ao

9 Tal sugestão tem repercussões nos artigos que trariam tais termos. Estas decorrências lógicas não foram compiladas como novas propostas.

mesmo tempo em que garanta a privacidade dos usuários".

Autor da proposta: *ABEP.*

(E) A possibilidade de "difusão" de dados pessoais deve ser vedada pela lei já em seu rol de definições.

"A transferência de dados a sujeitos indeterminados ["difusão"] *deve ser excluída da lei. É um absurdo que as pessoas sequer saibam com quem estão seus dados".*

Autor da proposta: *Gabriela Martins.*

(F) A possibilidade de "transferência internacional de dados" deve ser vedada pela lei já em seu rol de definições[10].

"A transferência internacional deveria ser vedada. Uma vez que o dado tenha sido transferido para outro país não há garantia nenhuma que ele tratará os dados com as mesmas obrigações, proteções e vedações que a lei brasileira. Em razão da soberania dos Estados, está é uma possibilidade perigosa" [*JCK*].

"Em razão da soberania dos Estados, esta por sugestão deveria ser excluída, pois o país que receber tais dados não dará garantia de segurança da lei brasileira" [*Tássia Martins*].

Autores da proposta: *JCK* e *Tássia Martins.*

(G) O conceito de transferência internacional de dados deve abarcar tanto o recebimento de dados quanto o envio.

Autor da proposta: *arns.*

Sugestões de redação:

Autores da sugestão: *Vivo.*

[MODIFICAÇÃO] XI - interconexão: tratamento de dados que consiste no relacionamento/cruzamento dos dados pessoais constantes de um ficheiro com os dados de um outro ficheiro ou ficheiros mantidos ou não pelo mesmo ou outro(s) responsável(is) com finalidade semelhante ou distinta;

10 Tal proposta teve uma oposição na plataforma por parte da participante *Giovanna Carloni*. Não consideramos uma "controvérsia" por que a intervenção foi antes uma crítica do que uma proposta alternativa.

4.4.13. Como deve ser definido o ato de "dissociação" de dados pessoais?

Neste inciso é possível observar que as contribuições dos participantes foram todas voltadas a tentar conciliar o conceito de dissociação com o de anonimização e, consequentemente, com o de dados anônimos.

Propostas avulsas para a regulação deste tema:

(A) A definição de "dissociação" deve fazer referência expressa da condição "anônima" dos dados "dissociados".

"Essa mudança garantiria que dados dissociados deixariam de ter a interpretação essencial à continuidade da inteligência de Big Data".

Autores da proposta: *ABRANET* e *Câmara BR.*

(B) O termo "dissociação" deve ser substituído por "anonimização[11]".

Os participantes defensores desta ideia sugerem a mudança do termo dissociação para anonimização. Segundo eles, a dissociação seria apenas uma das técnicas de anonimização de dados.

Também lembram que qualquer "anonimização" é reversível, e, portanto, não exclui o seu responsável por eventuais danos causados ao titular dos dados.

Autores da proposta: *GPoPAI, Joana Varon* e *Veridiana/Intervozes.*

(C) A lei deve trazer uma definição de "dissociação" que cite que tal processo "anonimiza" dados pessoais.

"Entendemos relevante que seja alterado o conceito de 'dissociação', para melhor compreensão de diversos trechos da Lei. Vale esclarecer que, a Constituição Federal, no inciso IV do artigo 5º, diz que é livre a manifestação do pensamento, sendo vedado o anonimato, para que se identifique o autor. Apesar de a privacidade ser protegida em nosso texto constitucional, o anonimato não o é, permitindo que os dados de cadastros e de conexões possam ser levantados através dos meios legais.

Diante disso, a anonimização de dados de tráfego de rede é o processo de retirar as informações que possam levar à identificação dos usuários da conexão. Mais abrangentemente, essa anonimização engloba também o conteúdo da informação trocada e também as informações que interferem na segurança da rede de origem e destino dos dados".

Autor da proposta: *Fiesp.*

[11] Partindo desta ideia, o *Article 29 Data Protection Working Party,* da União Europeia, publicou um documento, que deve ser levado em consideração no debate do anteprojeto, sobre a eficiência e os limites das distintas técnicas existentes de anomização. Este documento também faz a diferenciação entre os termos anomização (termo amplo) e dissociação (termo mais específico, uma das técnicas de anomização). Os participantes defensores desta proposta sugerem que a substituição ocorra nos seguintes pontos do anteprojeto de lei: Art 11, inc IV; Art 12 inc II-c; Art 15, inc II; Art 17, inc IV e paragrafo 5 e Art 50, inc III.

(D) A definição de "dissociação" deve incluir um "teste" que certifique que os meios utilizados foram razoáveis.

"Definição de dissociação deveria incluir o exame da razoabilidade com que estes dados possam ser reidentificados. Este exame deverá ter os seguintes critérios:(i) o incentivo ou falta de incentivo a uma sociedade de usar as informações para a identificação de uma pessoa natural, (ii) a facilidade / dificuldade para a identificação de uma pessoa natural, e (iii) a facilidade / dificuldade de obtenção de outros dados necessários para a identificação de uma pessoa natural".

Autor da proposta: *ITI.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] XIV - dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável, garantindo a anonimização;

Autor da sugestão: *ITI.*

[MODIFICAÇÃO] XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser razoavelmente associado, direta ou indiretamente, com um indivíduo identificado ou identificável;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] XIV – dissociação: ato de modificar o dado pessoal de modo que ele não possa ser associado esteja diretamente com um indivíduo identificado ou identificável;

4.4.14. Como deve ser definido o "bloqueio" de dados pessoais?

Os participantes que discutiram o conceito de bloqueio buscaram ou ampliar o conceito ou torná-lo mais restrito. Este tipo de sugestão é importante na medida em que pode ter impactos, por exemplo, na aplicação da sanção do inciso IV do artigo 50 ou no exercício de direitos do titular no inciso IV do artigo 17.

Propostas avulsas para a regulação deste tema:

(A) O "bloqueio" deve se restringir a atividades específicas, não ao tratamento em geral.

"Sugerimos que o bloqueio se restrinja a atividades específicas de tratamento, e não a toda e qualquer atividade de tratamento.

Isso porque nem todas as atividades podem ser suspensas temporariamente. Tem-se, por exemplo, a própria guarda dos dados por um operador, no caso do bloqueio temporário, o operador não pode ficar proibido de continuar guardando os dados, ainda que não possa trabalha-los durante o período da suspensão".

Autores da proposta: *Brasscom*.

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de determinadas operações de tratamento;

Autor da sugestão: *JCK.*

[MODIFICAÇÃO] XV – bloqueio: a suspensão de qualquer tipo de operação, consulta ou manipulação de dado pessoais armazenados em determinado escopo ou local;

4.4.15. A definição de "cancelamento" deve abranger apenas uma determinada base de dados?

Tal como no inciso anterior, em que se discutiu o conceito de bloqueio, a discussão acerca do conceito do cancelamento dividiu os participantes entre aqueles que apoiam que o cancelamento deve ser entendido de forma estrita, enquanto cancelamento em uma só determinada base de dados, e aqueles que entendem que o cancelamento deve ser entendido de forma mais ampla, como aquele realizado em todas as bases de dados.

A definição do conceito de cancelamento é muito importante frente aos reflexos que tal conceito pode causar, por exemplo, na imposição de sanções de acordo com o inciso VI do artigo 50 do anteprojeto ou mesmo do exercício de direitos do titular, do qual dispõe o artigo 17 em seu inciso IV.

Respostas controversas coletadas na plataforma de debate:

(A) Sim.

"*Acreditamos que este conceito deve ser lido de forma restritiva de forma a englobar o cancelamento*

dos dados apenas em determinada base de dados, não se exigindo a eliminação destes em toda rede de compartilhamento. Isso porque uma vez que os dados são compartilhados junto à rede resta quase impossível sua total erradicação".

Quem defendeu isso? *ABEMD*.

(B) Não, o cancelamento deve abranger todas as bases de dados.

O cancelamento deve ser a eliminação definitiva dos dados, em todos os lugares em que foram arquivados, incluindo cópias de *backup*. Ele deve impedir que os dados sejam acessados no futuro.

Há risco de os dados continuarem gravados digitalmente em outro formato ou em diversos pequenos pedaços a serem reunidos posteriormente com ajuda de softwares*12*.

Quem defendeu isso? *Giovanna Carloni, Veridiana/Intervozes, JCK* e *Joana Varon.*

(C) Não, porém o cancelamento não deverá se estender a bases de dados sob controle de outros responsáveis.

"Sugerimos que o conceito de cancelamento se aplique exclusivamente ao banco de dados que esteja efetivamente sobre controle do responsável pelo tratamento, sendo inviável que o responsável implemente a ação de cancelamento sobre banco de dados de outrem".

Quem defendeu isso? *Brasscom.*

Propostas avulsas para a regulação deste tema:

(A) O termo "cancelamento" deve ser substituído por "apagamento" ou "exclusão".

"Deve-se substituir o termo cancelamento pelo termo 'apagamento' ou pelo termo 'exclusão'. Isso porque 'cancelamento' pressupõe a ideia de término da relação de serviço".

Autores da proposta: *ABDTIC*.

Sugestões de redação:

Autor da sugestão: *Veridiana/Intervozes.*

[MODIFICAÇÃO] XVI – cancelamento: completa eliminação de dados ou conjunto de dados armazenados em banco de dados, inclusive de quaisquer copias de segurança que tenham sido previamente realizadas, seja qual for o procedimento empregado;

12 Ver exemplos em: <*http://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/*> ou <http://www.akdart.com/priv9.html>.

Autor da sugestão: *JCK.*

[MODIFICAÇÃO] XVI - cancelamento: a eliminação permanente de dado pessoal armazenados em determinado escopo ou local, inclusive de cópias de segurança previamente realizadas;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] XVI - cancelamento: eliminação, anonimização de dados ou do conjunto de dados armazenados em banco de dados, sob controle do responsável, e não se estende aos dados porventura replicados em outros locais sob controle de outras entidades;

4.4.16. Qual deve ser a definição legal de "uso compartilhado de dados"?

Propostas avulsas para a regulação deste tema:

(A) A definição deve ser ampliada para abranger "comunicação", "difusão", "transferência internacional de dados" e "interconexão".

"Deve-se expandir o conceito para abarcar as quatro formas de tratamento de dados (comunicação, difusão, transferência internacional e interconexão de dados) entre entes privados com entes privados. Posto que se trata de prática rotineira no mercado, observadas as exigências quanto ao consentimento dos titulares".

Autor da proposta: *Febraban*.

(B) O uso compartilhado de dados entre entes públicos e privados deve ter tutela especial.

Autor da proposta: *GPoPAI.*

(C) A definição deve falar de "cruzamento", não de "interconexão".

Autor da proposta: *ABDTIC.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] XVII -uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos, entes privados e entidades privadas, com autorização específica, para uma ou mais modalidades de tratamento; e

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] XVII - (...) para uma ou mais modalidades de tratamento delegados por esses entes públicos, mediante autorização do órgão competente nos termos do 24; e

4.4.17. Qual deve ser a definição legal de "encarregado", indicado pelo responsável pelo tratamento de dados pessoais?

Os comentários acerca da definição de encarregado foram todos no sentido de incluir a possibilidade de indicação, não de uma pessoa natural, mas de todo um setor em, por exemplo, uma empresa para que este atue como canal de comunicação.

Segundo os participantes, principalmente em grandes instituições, a indicação de um setor é mais eficiente e será mais capaz de atender a todas as demandas dos titulares e do órgão competente.

Propostas avulsas para a regulação deste tema:

(A) A definição de "encarregado" deve abranger a possibilidade de tal função são ser apenas desempenhada por uma pessoa natural.

Autores da proposta: *SindiTeleBrasil, Fiesp, Febraban* e *GSMA*.

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] XVIII - encarregado: pessoa física ou canal de atendimento, indicado pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] XVIII – encarregado: pessoa física ou jurídica, indicado pelo responsável, que atua como canal de comunicação perante os titulares, e que pode ser terceirizada.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] XVIII – encarregado: área ou departamento, indicado pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] XVIII – encarregado: pessoa natural ou área indicada pelo responsável, que atuará em seu nome, conforme disposto nesta Lei.

4.4.18. A lei deve trazer outras definições[13]? Quais?

Propostas avulsas para a regulação deste tema:

(A) A lei deve conter a definição de "dado reidentificado".

"Sugerimos a adição do conceito de dado reindetificado. A definição de "reidentificação" é importante para distinguir o dado que é efetivamente incapaz de identificação positiva daquele resultante do tratamento que o transforma em dado identificável"

Autor da proposta: *ABRANET* e *Câmara BR*.

(B) A lei deve conter uma definição que diferencie "dados cadastrais" de "dados pessoais" e "dados sensíveis".

Tal definição deixaria claro que dados cadastrais não abrange IP.

Autor da proposta: *Câmara BR.*

(C) A lei deve conter uma definição para a atividade de "pesquisa de mercado".

Segundo a *ABEP* isso garantiria a dissociação do tratamento de dados, necessária para a realização de pesquisas deste tipo, do tratamento comum realizado por empresas de *marketing* direto.

Autor da proposa: *ABEP.*

(D) A lei deve conter uma definição do "órgão competente".

"Recomenda-se a adição de inciso conceituando o órgão competente, de forma a mitigar os riscos jurídicos, já que o texto do anteprojeto fala diversas vezes em um 'órgão competente' sem, no entanto, defini-lo ou descrevê-lo".

Autor da proposta: *Fiesp.*

(E) A lei deve conter uma definição de "agentes de tratamento".

"A expressão 'agentes de tratamento' é mencionada em diversos artigos do Anteprojeto, tais como os artigos 10, 13, 17, 34, 36 e 43 e a definição deve ser inserida no artigo 5º por ser o local mais

13 A discussão sobre a definição de dados "de acesso público irrestrito" não foi abordada neste ponto. Por questões de organização ela foi exposta no artigo dedicado ao tema.

adequado para incluir tal definição".

Autor da proposta: *Febraban.*

(F) A lei deve conter uma definição de "interesse legítimo".

"O 'interesse legítimo' a que nos referimos e que aqui indicamos terá que ser: (a) um interesse legítimo do responsável ou de um terceiro a quem sejam fornecidos os dados (por exemplo, no caso do titular deixar de pagar determinada prestação a um banco e esse banco fornece os dados pessoais desse titular a uma empresa de cobrança para obter o pagamento da dívida pelo titular desses dados, ainda que o titular não tenha consentido), (b) esta exceção do interesse legítimo tem que respeitar os princípios de proteção de dados (princípio da qualidade dos dados e o princípio da necessidade e adequação, i.e., os dados têm que estar atualizados, e apenas serão transmitidos os dados necessários para a finalidade)".

Autor da proposta: *Vivo.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[INCLUSÃO] Novo inciso – dados cadastrais: dados de qualificação pessoal e identificação como nome, endereço físico e eletrônico, telefone, RG e CPF/CNPJ, sexo, profissão, filiação, naturalidade, nascimento, estado civil e óbito;

Autores da sugestão: *ABRANET* e *Câmara BR.*

[INCLUSÃO] Novo inciso - dado reidentificado: dado anônimo ou que tenha passado por processo de dissociação que o responsável submete a tratamento que lhe confira a capacidade de identificação do seu titular, no nível individual.

Autor da sugestão: *Fiesp.*

[INCLUSÃO] Novo inciso - órgão competente: órgão regulador-fiscalizador que seja definido na regulamentação.

Autor da sugestão: *Febraban.*

[INCLUSÃO] Novo inciso - agentes de tratamento de dados: responsável e o operador que realizam o tratamento de dados

Autor da sugestão: *Vivo.*

[INCLUSÃO] Novo inciso - interesses legítimos: sempre que existir interesse do responsável pelo tratamento ou do terceiro em efetuar um tratamento de dados lícito do titular, com o intuito de detectar ou prevenir fraudes, para garantir a segurança física ou lógica de sistemas, para assegurar atividades legítimas de gestão corrente das empresas ou autoridades, para garantir o

equilíbrio dos interesses em causa em determinada relação jurídica, tendo este interesse que: (i) estar de acordo com a presente Lei e as demais legislações vigentes no sistema jurídico brasileiro; (ii) ser um interesse real e atual; e (iii) ser um interesse claramente articulado para permitir garantir um teste de equilíbrio entre os interesses legítimos e os direitos fundamentais da pessoa em causa.

Autor da sugestão: *ABEP.*

[INCLUSÃO] Novo inciso - pesquisa de mercado: atividade empresarial regularmente exercida no Brasil, em estrito cumprimento da legislação brasileira, que inclui pesquisas de mercado, sociais, de mídia e de opinião, consistente na coleta sistemática e a interpretação de informações sobre indivíduos ou organizações utilizando-se métodos e técnicas estatísticos e analíticos das ciências sociais aplicadas para obter conhecimentos ou dar suporte ao processo de tomada de decisões. No âmbito de tais atividades a identidade dos entrevistados não será revelada ao usuário das informações sem consentimento explícito e nenhuma abordagem de vendas será feita aos entrevistados como resultado direto de terem fornecido informações.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive ~~a partir de~~ números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

II – tratamento: ~~conjunto de ações referentes~~ toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, ~~transporte,~~ processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, ~~bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão,~~ transferência, difusão ou extração;

III – dados sensíveis: dados pessoais ~~que revelem~~ sobre a origem racial ou étnica, as convicções religiosas, ~~filosóficas ou morais,~~ as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos;

IV – dados ~~anônimos~~ anonimizados: dados relativos 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 para identificar o referido titular~~;

V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;

VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;

VII – consentimento: manifestação livre~~, expressa, específica~~ e inequívoca ~~informada~~ pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;

~~**X** – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;~~

~~**XI** – interconexão: transferência de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;~~

~~**XII** – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma;~~

X – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

XI – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;

XII – ~~dissociação~~ anonimização: ~~ato de modificar o~~ qualquer procedimento por meio do qual um dado ~~pessoal~~ deixa de ~~modo a que ele não possa~~ poder ser associado, direta ou indiretamente, ~~com~~ a um indivíduo ~~identificado ou identificável~~;

XIII – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XIV – ~~cancelamento~~ eliminação: ~~eliminação~~ exclusão definitiva de dado~~s~~ ou de conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

XV – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e

4.5. Princípios gerais para o tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:

I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular;

II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades almejadas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

III – princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

IV – princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;

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;

VI – princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;

VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

§ 1º Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.

§ 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.

4.5.1. Propostas gerais sobre os princípios para o tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve harmonizar os princípios gerais do artigo 6º com os princípios constitucionais que balizam a livre atividade econômica.

"A legislação que trata da proteção de dados pessoais deve conter permissão expressa e não condicionada ao consentimento do titular a coleta e tratamento de dados pelas empresas gestoras dos cadastros de proteção ao crédito (as quais são qualificadas como entidades de caráter público em virtude do quanto disposto no art. 43, § 4º do CDC) em seus produtos e serviços, atendidos os princípios da finalidade, adequação, necessidade, segurança e transparência, e respeitados os assim considerados dados sensíveis"

Autor da proposta: *Boa Vista Serviços*.

(B) Princípios deste artigo devem ser conceituados de maneira mais objetiva, de forma a evitar repetições desnecessárias.

Autor da proposta: *Fiesp.*

4.5.2. O princípio da finalidade deve ser flexibilizado? Como?

Com exceção da MPA, que fez um comentário acerca do combate a atividades ilícitas (que será tratado no final), todos os comentários neste inciso argumentam em favor de uma maior flexibilização do princípio da finalidade.

As alterações sugeridas têm uma diferença sutil, enquanto todos concordam que as finalidades não devem ser "específicas, explícitas e conhecidas", eles discordam quanto qual deva ser a nova qualificação da finalidade.

De um lado, houve quem argumentou que a finalidade poderia ser tão somente esperada pelo titular, ou seja, dentro de suas expectativas; de outro, houve quem argumentou a favor da necessidade de informar devidamente o usuário.

Propostas avulsas para a regulação deste tema:

(A) Os termos "específicas, explícitas e conhecidas" devem ser substituídos por "devidamente informadas".

A mudança seria adequada pois *"propósito surge durante o processamento de dados"*. A justificativa

é a abertura para inovação no uso dos dados possibilitada pela reconfiguração do princípio.

Autores da proposta: *CNseg, Câmara BR, ABRANET* e *Brasscom.*

(B) O princípio deve abranger finalidades "esperadas", não apenas "conhecidas".

A justificativa é pelo "crescimento econômico", com as mesmas bases argumentativas "pró-inovação" apresentadas na proposta (A).

Autores da prosposta: *ABA, GSMA, ITI, Febraban, Centre for Information Policy Leadership* e *CNI.*

(C) O princípio da finalidade deve ter uma exceção para combate à fraude e atividades ilegais praticadas na Internet.

"Sugerimos o acréscimo de uma exceção ao princípio da finalidade. Isso porque, em se tratando de evitar fraude e atividades ilegais praticadas online, tais quais a lavagem de dinheiro e a pirataria, as autoridades públicas e os provedores de conexão e de aplicação devem ter a prerrogativa de coletar e tratar dados pessoais independentemente da permissão do indivíduo envolvido.

Obviamente, agentes interessados em atividades ilícitas não darão seu consentimento para o tratamento de dados que pode prejudicar suas condutas ilegais".

Autor da proposta: *MPA.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades devidamente informadas ao titular;

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas devidamente informadas, pelo titular;

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] I - princípio da finalidade, pelo qual dados pessoais devem ser obtidos e processados com finalidades específicas e legítimas, desde que estejam dentro da razoável expectativa do titular;

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] I - princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas e conhecidas pelo titular;

Autor da sugestão: *Centre for Information Policy Leadership.*

[MODIFICAÇÃO] I – princípio de finalidade, pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas e explícitas que sejam conhecidas, ou razoavelmente esperadas, pelo titular, considerando o contexto do tratamento;

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] I - princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular, exceto quando a coleta e tratamento de dados se der no intuito de proteger direitos, evitando fraude e atividades ilegais;

4.5.3. Princípio da adequação: debates sobre "finalidade almejada" e "legítima expectativa"

Os debates sobre o princípio da adequação giraram em torno da incerteza quanto aos conceitos de "finalidade almejada" e "legítima expectativa". A falta de critérios para entender estas disposições foi, inclusive, alvo de indagações pela *ABEMD* e pelo *Centre for Information Policy Leadership*. Segundo levantamento, duas propostas foram identificadas endereçando tais critérios. Paralelamente, o *Centre for Information Policy Leadership* sugeriu a inclusão de uma "exceção" para casos em que não houver compatibilidade entre as finalidades almejadas e as expectativas do titular.

Propostas avulsas para a regulação deste tema:

(A) A expectativa do titular deve estar associada ao consentimento dado por ele ao responsável pelo tratamento[14].

Autores da proposta: *SindiTeleBrasil.*

(B) O princípio da adequação deve ordenar que o tratamento seja compatível com a finalidade informada ao titular.

Segundo os participantes que defenderam essa proposta, o tratamento deve ser compatível com a finalidade informada ao titular, e não com a finalidade almejada ou com suas legítimas expectativas. O conceito de "almejadas e com as legítimas expectativas" seria muito subjetivo, pois o titular poderia 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.

[14] O *SindiTeleBrasil* inseriu a mesma proposta na discussão a respeito do "princípio da necessidade".

Autores da proposta: *CNseg* e *US Business Council.*

(C) O princípio da adequação deve prever uma exceção em favor do tratamento de dados com fundamento no "interesse legítimo" do titular.

"Para garantir a correta interpretação do que é uma finalidade compatível, é recomendável incluir algumas orientações adicionais sobre os fatores que os responsáveis devem levar em conta ao determinar se uma finalidade posterior é compatível ou não. Este é o tratamento adotado na Europa".

Autor da proposta: *Centre for Information Policy Leadership.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades consentidas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] 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;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

4.5.4. Princípio da necessidade: como definir que um tratamento foi o "mínimo necessário"?

Nesse inciso, o conteúdo da crítica levantada pelo ITI foi o mesmo conteúdo utilizado nas sugestões de mudança recebidas por este inciso.

Segundo o ITI, a limitação ao "mínimo necessário" seria subjetiva, razão pela qual não poderia ser considerada no melhor interesse dos consumidores. Os demais participantes procuraram sugerir uma alternativa para a ideia de "mínimo necessário".

Propostas avulsas para a regulação deste tema:

(A) O termo "mínimo" deve ser substituído por "razoavelmente" na redação do princípio da necessidade.

Esta proposta contemplaria situações nas quais o tratamento não é exigido, mas é recomendável ou útil para benefícios do usuário, como, por exemplo, em questões de segurança de sistemas ou para o fornecimento de serviços avançados ou compatíveis.

Autores da proposta: *Câmara BR, Brasscom* e *ABRANET.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] III - princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades consentidas, abrangendo dados pertinentes, proporcionais e não excessivos;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] III – princípio da necessidade, pelo qual o tratamento deve se limitar ao que for razoavelmente necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] III – princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo razoavelmente necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

4.5.5. Princípio do livre acesso

Propostas avulsas para a regulação deste tema:

(A) O princípio do livre acesso deve ter uma limitação de "razoabilidade" para circunstâncias nas quais o acesso não seja viável.

Autores da proposta: *ITI.*

(B) Não deve ser garantida a consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento dos dados.

"*Isso porque conhecer a modalidade de tratamento dos dados não traz benefício aos titulares. Além disso, a modalidade fica a critério do responsável e, muitas vezes, pode configurar em estratégia*

empresarial".

Autor da proposta: *Febraban.*

(C) Deve ser garantido ao titular o acesso à integralidade de seus dados pessoais de um banco de dados específico.

Autor da proposta: *Boa Vista Serviços.*

(D) O princípio do livre acesso deve conter o dever do responsável em apagar ou corrigir dados incompletos ou incorretos.

Autor da proposta: *Privacy International.*

(E) O princípio do livre acesso deve ser suprimido, pois ele já está contemplado no princípio da transparência.

Autor da proposta: *ABRANET.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] IV - princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre a integralidade dos seus dados pessoais;

4.5.6. Princípio da qualidade dos dados: responsabilidade e atualização

Neste inciso, o principal debate ocorreu em relação a responsabilidade das empresas quanto a exatidão, clareza e, principalmente, atualização dos dados[15]. Além disso, foram levantadas pelo *ITI* hipóteses em que responsáveis pelo tratamento serão obrigados a manter dados incorretos em seus bancos.

Quem deve ter a responsabilidade de manter exatos, claros e atualizados os dados pessoais?

15 O participante *Roberto Taufick* apontou uma necessidade de discussão mais profunda sobre a ideia de "atualização" ou "atualidade". Segundo ele "*há necessidade de definir o conceito de 'atualidade'.* (...). É *a partir dele que o* 'right to be forgotten'*, ou* 'derecho al olvido' *poderá ser lido na nossa legislação. Na Europa e na Argentina existe a possibilidade de apagar qualquer dado a pedido do interessado. Isso leva a desajustes, como foi a decisão no caso Google Spain (*'right to be forgotten'*), em que a informação pública (publicada pelo Ministério do Trabalho espanhol) não poderia ser replicada pelo Google -- apesar de a informação ser válida, estar disponível na origem (na página eletrônica e na veiculação impressa do DOU espanhol) e poder ainda ser encontrada por outros mecanismos de busca sem poder de mercado na Europa, como Yahoo*".

Respostas controversas coletadas na plataforma de debate:

(A) Esta responsabilidade não deve existir.

"Sugerimos nova proposta de redação tendo em vista que as empresas não devem ser responsabilizadas pela veracidade ou atualização dos dados coletados de terceiros. Elas apenas devem ser responsabilizadas pela integridade dos mesmos, ou seja, por disponibilizar e guardar de maneira clara todos os dados fornecidos, sem risco de danos".

Quem defendeu isso? *Câmara BR, Boa Vista Serviços, Brasscom* e *ABRANET.*

(B) Esta responsabilidade deve se limitar ao oferecimento de mecanismos para que os titulares efetuem as atualizações. Não há responsabilidade se não há conhecimento sobre a desatualização.

"Pode haver alguns casos onde o titular dos dados fique responsável por fornecer dados atualizados e seria inadequado ou indesejável para terceiros buscar atualizações de maneira proativa ou exigir a verificação dos dados fornecidos.

Desta forma, sugerimos uma alteração no o texto para indicar que, em determinadas circunstâncias, os terceiros recebendo tais informações devem ser responsáveis por manter em funcionamento todos os processos e sistemas que possam ser necessários para permitir tal atualização"

Quem defendeu isso? *US Business Council* e *CNseg.*

(C) Esta responsabilidade deve se limitar à manutenção e atualização, excluída hipótese de fraude, erro, culpa ou dolo do titular dos dados.

Quem defendeu isso? *SindiTeleBrasil*

(D) Esta responsabilidade deve ser conferida ao titular dos dados pessoais.

"A responsabilidade de atualizar os dados deve ser do seu titular, em períodos previstos em lei. Considero este inciso um dos mais importantes para a efetiva aplicação da lei, pois pretende garantir que os dados pessoais sejam atualizados na medida em que for necessário.

Mas para garantir maior eficiência, a responsabilidade em manter atualizados os dados devem ser do titular, e esse deverá informar qualquer mudança que ocorra em períodos a ser especificado pela lei. A lei também deve garantir um modo rápido e de fácil acesso para que seja feita esta atualização".

Quem defendeu isso? *Lucas Nascimento.*

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever exceções ao princípio da qualidade dos dados com a finalidade de

prevenir fraudes ou proteger direito de terceiros.

"Existem circunstâncias nas quais seria necessário que a organização mantivesse informações incorretas. Para prevenção de fraudes, seria necessária a manutenção de informações incorretas mesmo se essas informações fossem corrigidas. Ainda, essa disposição deveria permitir exclusões se as informações ou suas correções infringissem direitos de terceiros ou estivessem relacionadas aos dados sob o controle de outra parte (uma pessoa natural ou jurídica), ou se obrigatórias por contrato ou se devam ser mantidas por outra pessoa jurídica.

Além do mais, cabe ressaltar que qualquer obrigação de manter dados corretos deveria ser comensurada ao objetivo para o qual os dados devam ser usados e ao risco para a pessoa natural se de fato os dados não estiverem corretos".

Autor da proposta: *ITI.*

Sugestões de redação:

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] V - princípio da qualidade dos dados, pelo qual devem ser presumidas a exatidão, a clareza e atualização dos dados informados pelo titular, admitindo-se prova em contrário e atualização de acordo como a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] 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;

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão e a clareza, conforme fornecido pelo seu titular e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, ou, nos casos onde o titular for responsável pelo fornecimento dos dados, um processo é colocado em funcionamento para permitir tais atualizações, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] V – princípio da qualidade dos dados, pelo qual deve ser garantida a integridade

dos dados tais como fornecidos, para cumprir os seus respectivos efeitos de tratamento legalmente autorizado;

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] V – princípio da qualidade dos dados, pelo qual devem ser garantidas integridade dos dados, coletados para cumprir os seus respectivos efeitos de tratamento legalmente autorizado;

4.5.7. Princípio da transparência

Propostas avulsas para a regulação deste tema:

(A) O princípio da transparência deve considerar os direitos de propriedade intelectual dos operadores de tratamento dos dados.

"Tendo em vista os benefícios vindouros do Big Data, este princípio deve ser aplicada de maneira a honrar os direitos concernentes à propriedade intelectual dos operadores de dados. É verdade quem algum nível de transparência é necessário para evitar quebras de expectativa quanto ao tratamento, no entanto, este nível de transparência não deve incluir publicação compulsória de algoritmos protegidos por propriedade intelectual".

Autor da proposta: *ABA.*

(B) O princípio da transparência deve ser substituído por deveres objetivos específicos.

"Mais efetivo talvez que um princípio de transparência que traz uma obrigação genérica de manter dados claros etc, seria ter um provisão de que as empresas devem fornecer uma notificação ou termos de uso com linguagem clara e acessível que identifique: (i) as regras de privacidade e segurança adotadas; (ii) quais dados coletados/ utilizados, incluindo as fontes de onde foram retirados esses dados; (iii) o propósito pelo qual coleta/utiliza dados; (iv) quem são as pessoas que têm acesso a tais dados (em caso de dados compartilhados); (v) por quanto tempo esses dados serão mantidos; (vi) quis medidas são tomadas para assegurar a proteção do dados coletados e (vi) quem o usuário deve contatar/ reclamar em caso de dúvidas/ preocupações quanto a coleta de dados".

Autora da proposta: *Daniele Fontes.*

4.5.8. Princípio da segurança

Propostas avulsas para a regulação deste tema:

(A) O princípio da segurança dos dados deve ser balizado pelos "padrões adotados pela indústria", não por um dever de atualização.

"Sugerimos a eliminação da expressão 'constantemente atualizadas' e a inserção da redação 'medidas técnicas e administrativas compatíveis com os atuais padrões adotados pela indústria'. A

necessidade de atualização constante se mostra um ônus muito elevado para as empresas, medidas de segurança compatíveis com o 'atual estado da tecnologia' não ficam disponíveis no mercado a preços acessíveis. Dessa forma, a exigência de padrões industriais se apresenta muito mais razoável.

Além do mais, a exigência de atualizações constantes contradiz o próprio texto do Art. 47, que permite ao órgão competente a criação de regras baseadas na evolução tecnológica".

Autor da proposta: *MPA.*

(B) O dever de atualização de medidas técnicas e administrativas de segurança deve ser relativizado, pois algumas tecnologias precisam ser atualizadas com mais frequência que outras.

Autor da proposta: *ITI.*

(C) O princípio da segurança deve explicitar que a segurança dos dados necessita de medidas físicas e eletrônicas.

Autor da proposta: *3M do Brasil.*

Sugestões de redação:

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] VII - princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas compatíveis com os atuais padrões adotados pela indústria, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Autor da sugestão: *ITI.*

[MODIFICAÇÃO] VII - princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas proporcionais à evolução dos riscos e à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Autor da sugestão: *3M do Brasil.*

[MODIFICAÇÃO] VII - princípio da segurança, pelo qual devem ser utilizadas medidas técnicas, físicas e eletrônicas, e administrativas proporcionais à evolução dos riscos e à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

4.5.9. Princípio da prevenção

Propostas avulsas para a regulação deste tema:
(A) O princípio da prevenção deve ser suprimido, pois já é abarcado pelo princípio da segurança. **Autor da proposta:** *SindiTeleBrasil.*
(B) A definição legal do princípio da prevenção deve trazer rol exemplificativo de boas práticas **Autor da proposta:** *Tatiana Ferreira* e *RafaeIC.*

4.5.10. Princípio da não discriminação

Propostas avulsas para a regulação deste tema:
(A) O princípio da não discriminação não deve vedar discriminação que garanta isonomia ou discriminação positiva. **Autores da proposta**[16]**:** *ABEMD, CNseg, Câmara BR, Brasscom, ITI* e *ABRANET.*
(B) O princípio da não discriminação não deve vedar a classificação ou separação de informações. *"Este princípio não deve impedir que através do tratamento sejam diferenciados ou distintos determinados grupos ou informações. Deve excepcionar-se discriminar no sentido de "separar" ou "classificar", de discriminar no seu sentido pejorativo ou relacionado a informações sensíveis (assim entendidas nos termos do art.5º, III do APL)".* **Autor da proposta:** *Boa Vista Serviços.*
(C) O princípio da não discriminação deve vedar apenas a discriminação por orientação religiosa, política, por origem racial ou étnica, ou participação em movimentos sociais.

16 Os participantes *Câmara BR, Brasscom, ITI* e *ABRANET* acreditam que a única discriminação que deva ser vedada seja aquela que pode ser enquadrada como ilícita. *CNseg* argumentou no mesmo sentido: "*a discriminação com base em dados pessoais é razoável em diversas atividades que exigem a definição de um perfil de cliente para analisar os riscos, tais como análise a definição de um perfil de cliente para analisar os riscos, tais como análise de crédito e de seguros* (...)[s]*ugere-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*".

Autor da proposta: *GSMA.*

(D) O princípio da não discriminação não deve vedar o uso de dados em tomadas de decisão de forma genérica.

Autor da proposta: *ABA.*

Sugestões de redação:

Autor da sugestão: *Câmara BR* e *Brasscom.*

[MODIFICAÇÃO] IX – o princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios ilícitos;

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] IX – princípio da não discriminção, pelo qual o tratamento não pode ser realizado para discriminar indivíduos por orientação religiosa ou política, origem racial ou étnica, ou por participação em movimentos sociais;

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] 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;

4.5.11. Dever de publicidade de atividades de tratamento de dados dos órgãos públicos

Propostas avulsas para a regulação deste tema:

(A) O dever de publicidade de atividades de tratamento de dados deve ser aplicável a entidades privadas.

Autores da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 6º (...) §1º As pessoas jurídicas de direito público e privado darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.

4.5.12. Aplicação dos princípios de finalidade, adequação e necessidade ao uso compartilhado de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A aplicação deve se estender ao "tratamento" compartilhado.

Autor da proposta: *SindiTeleBrasil.*

(B) A aplicação de princípios gerais da lei à administração pública não deve se limitar apenas à finalidade, adequação e necessidade. Todos os princípios elencados devem ser respeitados.

Autores da proposta: *Giovanna Carloni, Lucas Zolet* e *ABRANET.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 6º (...)§ 2º O tratamento compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III e ressalvadas as demais disposições legais relativas a garantia do sigilo dos dados.

4.5.13. Existem outros princípios que devem ser positivados na lei?

Propostas avulsas para a regulação deste tema:

(A) A lei deve conter o princípio da "privacidade desde a concepção" (*privacy by design*).

"Privacidade desde a concepção: O art. 6º poderia fazer menção direta à aplicação do princípio de privacidade desde a concepção, reforçando a política protetiva da lei ao adiantar a preocupação com a proteção de dados pessoais desde momento inicial da elaboração de ferramentas e medidas

organizacionais que podem impactar em sua esfera".

Autor da proposta: *CTS-FGV.*

(B) A lei deve conter o princípio da "privacidade como padrão" (*privacy by default*).

"Privacidade como padrão: princípio pelo qual as configurações de privacidade dos produtos ou serviços devem ser as mais protetivas possíveis, considerando os estritos fins que legitimaram a coleta de dados, tanto em aspectos técnicos como organizacionais, sendo facultado ao usuário alterá-las para padrões mais públicos".

Autor da proposta: *CTS-FGV.*

(C) A lei deve conter o princípio da "legalidade e equidade na obtenção e processamento de dados".

Este princípio combateria transferências e vendas de dados fraudulentas.

Autor da proposta: *Privacy Information.*

(D) A lei deve conter um princípio que conceda ao titular o direito de retirar o seu consentimento, a qualquer momento.

Autor da proposta: *Flávio Costa.*

(E) A lei deve conter um princípio que prestigie a liberdade de iniciativa.

Autor da proposta: *ABRANET.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 6º As atividades de tratamento de dados pessoais deverão ~~atender aos~~ observar a boa-fé e seguintes princípios ~~gerais~~:

I – ~~princípio da~~ finalidade, pelo qual o tratamento deve ser realizado ~~com~~ para finalidades legítimas, específicas, explícitas e ~~conhecidas pelo~~ informadas ao titular;

II – ~~princípio da~~ adequação, pelo qual o tratamento deve ser compatível com as suas finalidades ~~almejadas~~ e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

III – ~~princípio da~~ necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades ~~almejadas~~, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – ~~princípio do livre~~ acesso~~,~~: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita ~~pelos titulares~~ sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;

V – ~~princípio da~~ qualidade dos dados~~,~~: pelo qual devem ser garantidas aos titulares a exatidão, a clareza, a relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI – ~~princípio da~~ transparência~~,~~: pelo qual devem ser garantidas aos titulares informações claras ~~e~~, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

VII – ~~princípio da~~ segurança~~,~~: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – ~~princípio da~~ prevenção~~,~~: pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX – ~~princípio da~~ não discriminação~~,~~: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

~~**§ 1º** Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.~~

~~**§ 2º** O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.~~

4.6. Consentimento como requisito para o tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

CAPÍTULO II – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I – Consentimento

> **Art. 7º** O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.
>
> **§ 1º** O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.
>
> **§ 2º** É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.
>
> **§ 3º** O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.
>
> **§ 4º** O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.
>
> **§ 5º** O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.
>
> **§ 6º** O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.
>
> **§ 7º** São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.
>
> **§ 8º** Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

O consentimento é o pilar regulatório adotado para a proteção de dados pessoais. A regra geral é a de que o cidadão deve consentir para que haja fluxo de suas informações pessoais, sendo essa a razão da extensa adjetivação empregada como: livre, expresso, específico e informado.

É curioso notar que as contribuições têm um traço comum crítico construtivo sobre essa estratégia regulatória. No entanto, o saldo regulatório final delas rivaliza-se para limitar ou fortalecer a regra do consentimento, havendo um embate quanto: *(i)* à adjetivação do consentimento; *(ii)* a novas formas para operacionalizar o consentimento; e *(iii)* à necessidade de haver novas exceções à regra do consentimento e como elas deveriam ser internalizadas.

Nesse contexto, o mapeamento das contribuições procurará captar essa tensão do debate público. Para tanto, mostrou-se necessário, por vezes, inverter a ordem sequencial dos

dispositivos comentados para, justamente, facilitar a compreensão desses embates gerados na plataforma, conectando-os um ao outro. Por isso, ao lado das propostas há uma observação dos dispositivos envolvidos no debate da consulta pública.

4.6.1. Vedação do tratamento de dados pessoais cujo consentimento foi obtido mediante erro, dolo, estado de necessidade ou coação

Propostas avulsas para a regulação deste tema:

(A) A vedação do tratamento em caso de erro na obtenção do consentimento deve ser suprimida por estar abarcado pelo direito geral de revogação do consentimento.

"Como a lei já garante o direito de revogação caso o titular tenha incorrido em erro, acreditamos que esse termo deve ser retirado desse parágrafo".

Autores da proposta: *Câmara BR*

(B) Deve haver uma vedação geral ao tratamento de dados obtidos de forma ilícita.

Segundo a *ABRANET,* o erro não deve ser uma vedação ao tratamento dos dados. No caso de um erro de consentimento, todo o tratamento dos dados apresentados antes da comunicação do erro não deveria ser considerado como indevido. A lei já garantiria o direito de revogação, caso o titular tenha incorrido em erro. A associação defende que o dolo, estado de necessidade e a coação seriam melhor abordados de uma forma genérica.

Autores da proposta: *ABRANET.*

Sugestões de redação:

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] §2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido de forma ilícita.

4.6.2. A adjetivação imposta ao consentimento deve ser restringida ou ampliada?

Respostas controversas coletadas na plataforma de debate:

(A) Deve ser restringida.

A.1. Excluindo-se todos os adjetivos [artigo 5°, inciso VII, e 7°, caput] (*Câmara BR)*

A eliminação dos adjetivos diminuirá o risco de conflitos, devendo-se analisar, casuisticamente, se há um consentimento inequívoco a legitimar o tratamento dos dados pessoais. Isso evitaria, sobretudo, uma redundância do termo consentimento.

A.2. Substituindo-se o adjetivo expresso pelo termo inequívoco: hipótese de consentimento implícito [artigo 5°, inciso VII, e 7°, caput] (*Mariana Cunha e Melo, Claro, Centre for Information Policy Leadership, ITI, Febraban, CNI, Marlon, BSA, ITS-Rio, US Business Council, Fiesp, IAB, ABRANET, Boa Vista Serviços* – essa última entende o consentimento expresso não é a mesma coisa que o sistema opt-in[17]*)*

Essa definição (consentimento expresso) criaria um sistema inflexível em que seria necessária colher a todo momento e previamente o consentimento do titular dos dados pessoais (opt-in) (*Mariana Cunha e Melo*). Essa hipótese não beneficiaria nem mesmo os consumidores, porque eles seriam sobrecarregados com uma série de notificações, fadigando, em última análise, a sua própria capacidade de controlar seus dados pessoais (*Claro e Centre for Information Policy Leadership*). Por isso, tal adjetivo deveria ser substituído pelo termo inequívoco para dar margem a um sistema de autorizações (consentimento) implícito (*GSMA*). Isso permitiria que os dados fossem utilizados, de forma contextual, de acordo as expectativas de cada relação jurídica (*US Business Council*). Deve ser ressalvado, no entanto, a existência de mecanismos que possibilitem o acesso, correção, bloqueio ou mesmo cancelamento de tais práticas com os dados pessoais (opt-out) (*ITS-Rio, BSA*). Dessa forma, não seria engessada uma série de inovações em que seria impraticável colher o consentimento de todos os titulares dos dados pessoais.***18***

A.3. Excluindo-se a exigência de consentimento específico [artigo 5°, inciso VII, e 7°, caput e §5°] (*Mariana Cunha e Melo, CTS-FGV, Câmara BR, MPA, Brasscom, Febraban, ABRANET, Febraban, ESA, US Business Council, ABRANET, CNI, Centre for Information Policy Leadership, ITI, SindiTeleBrasil, ABDTIC)*

Seria impossível prever todas as variações e possibilidades de tratamento de dados pessoais. Esse é, exatamente, o estado atual da arte da tecnologia que, com o advento do Big Data, mostra-se incompatível com relação à exigência de um consentimento específico (*Maria Cunha e Melo*). Nesses casos, o responsável pelo tratamento não pode definir - ou até mesmo ter uma compreensão clara - da finalidade do processamento dos dados no momento ou antes da coleta inicial e (*CTS-FGV, Centre for Information Policy Leadership*). Logo, essa exigência seria, extremamente, inviável e prejudicial para as inúmeras atividades comerciais que estão sendo conduzidas por essa potencialidade imprevisível da inovação lastreada no tratamento dos dados pessoais.

A.4. O princípio do consentimento deve ser interpretado/aplicado, restritivamente, quando os dados pessoais forem indispensáveis (adjetivo) para o fornecimento de um produto ou serviço [artigo 7°, caput e §1°] (*ABEMD, Câmara BR, Brasscom, ITI e ESA, MPA – esse último propõe, inclusive, a supressão do artigo 7°,§1°)*

Muitos modelos de negócio têm como sua base de sustentação econômica o tratamento de dados pessoais (*ABEMD*). Assim sendo, o consentimento não pode ser obstáculo para a operacionalização dessas atividades comerciais, sob pena de inviabilizar, economicamente, tais atividades comerciais (*MPA*). Até, por isso, seria melhor que a palavra indispensável fosse

[17] Vale ressalvar que alguns proponentes são dissidentes com relação à completo exclusão do consentimento expresso, o qual sobreviveria para a hipótese dos dados sensíveis [GSMA], ou, analogamente, naquelas hipóteses em o tratamento dos dados apresentariam sérios riscos [*ITI* e *Centre for Information Policy Leadership*].

18 Nota: a discussão sobre a possibilidade do consentimento implícito está, diretamente, ligada com a criação de uma nova hipótese para a dispensa do consentimento (interesses legítimos). Nessa questão, percebe-se que há uma certa dissidência desse grupo de proponentes conquanto à ampliação/restrição dessa cogitada nova exceção ao consentimento.

substituída por necessário, já que os dados pessoais podem não ser imprescindíveis para o funcionamento de uma aplicação, mas, são, certamente necessário para a viabilização do modelo de negócios (*ESA, Febraban*).

A.5. A sua revogabilidade poderá implicar na perda da gratuidade de serviços e produtos para os quais os dados pessoais são necessários e não deverá prejudicar os dados coletados e tratados anteriormente a sua revogação [artigo 7°, caput e §6°]***19***

> Mesmo que o consentimento seja revogável a qualquer momento, sem que haja qualquer tipo de ônus para o titular dos dados pessoais, deve-se observar que tal pedido poderá ter algumas implicações/restrições:
> a) perda da gratuidade de alguns serviços com a revogação do consentimento (*Câmara BR*). Isto porque, para alguns serviços e produtos os dados pessoais, ora objeto consentimento, são indispensáveis para a regular prestação do serviço, de modo que o usuário poderá ser alertado sobre a possibilidade de haver interrupção ou perda do serviço (*GSMA*). Caso contrário, isso traria enorme insegurança jurídica para os serviços e produtos de online gratuitos (*Brasscom*) ou mesmo para outros tipos de relações jurídicas em que os dados pessoais são necessários para a correta prestação de um serviço (*CNseg*). (*Câmara BR, GSMA, Brasscom, US Business Council, CNseg e ABRANET, ITI)*
> b) O tratamento realizado pelo responsável anteriormente à data de revogação do consentimento do titular não poderá ser prejudicado. Isso significa que tais dados não poderão ser deletados, podendo ser mantidos pelo responsável pelo atividade de tratamento dos dados pessoais. (*US Business Council, Febraban, Fiesp, CNSeg*)

Quem defendeu isso? *Mariana Cunha e Melo, CTS-FGV, Câmara BR, MPA, Brasscom, Febraban, ABRANET, Febraban, Fiesp, IAB, BSA, ITS-Rio, Marlon, ESA, US Business Council, ABRANET, CNI, Centre for Information Policy Leadership, ITI, SindiTeleBrasil, ABDTIC, Boa Vista Serviços.*

(B) Deve ser ampliada.

B.1. Prevendo-se a hipótese de consentimento granular (adjetivo), possibilitando-se uma esfera de controle mínima dos dados pessoais nos casos em que eles sejam indispensáveis para a prestação de um serviço/produto [artigo 5°, inciso VII, e 7°, caput e §1°] (*Margareth, Kacsavio, Gleison Melo, RafaelC., Veridiana/Intervozes, GPoPAI, Fiesp*)

> Deve ser, expressamente, permitido ao titular delimitar quais dados estarão submetidos à atividade de tratamento (*Margareth*). Ele deveria, portanto, ter um maior poder de decisão sobre as suas próprias informações (*Kacsavio*). Isso porque, o consentimento deverá ser fornecido, escalonadamente, a depender do contexto (*RafaelC.*). É a ideia do chamado "controle granular" que permite ao titular dos dados autorizar parte da coleta e do tratamento de acordo com os seus interesses na utilização de um determinado produto ou serviço (*GPoPAI, Veridiana/Intervozes*), rompendo com a lógica de que se deve aceitar tudo ou não aceitar nada das políticas de privacidade (*Fiesp*). Por exemplo: (i) quais os tipos de dados pessoais serão coletados (geolocacionais, referentes ao seu estado de saúde e etc.); (ii) a quais tipos de tratamento seus dados pessoais estarão sujeitos (para a entrega de conteúdo e/ou publicidade direcionada, para ativar determinadas funcionalidades de um aplicativo mobile e etc.); (iii) por quanto tempo e frequência durará o tratamento de suas informações pessoais (*GPoPAI*).

B.2. Prevendo-se que o consentimento seja renovado (adjetivo), caso surjam novas finalidades para o tratamento dos dados pessoais [artigo 5°, inciso VII, e 7°, caput e §5°] (*GPoPAI e Marlon [esse participante defende que o consentimento tácito deveria ser, expressamente, proibido pela lei])*

> Deve ser previsto, expressamente, que o consentimento deve ser renovado a cada nova finalidade surgida para o tratamento de dados pessoais. Ou seja, quando houver uma mudança

19 Nota: a discussão sobre a revogabilidade do consentimento está, diretamente, ligada a inclusão do direito de portabilidade que foi objeto de sugestões ao artigo 17.

de condições no contrato ou serviço, isso deve implicar, obrigatoriamente, a renovação do consentimento com a prestação das devidas informações ao usuário (*Marlon*).

B.3. A revogabilidade (adjetivo) do consentimento deve garantir a exclusão de todos os dados coletados [artigo 7°, caput e §6°] (*Privacy Information)*

A revogação do consentimento deverá implicar na exclusão de todos os dados coletados.

Propostas avulsas para a regulação deste tema:

(A) A lei deve autorizar a coleta de autorizações genéricas de dados pessoais ou definir o que isso significa.

Na linha da discussão anterior, parte dos proponentes posicionaram-se no sentido de que deveria ser: a) excluída a proibição de colher autorizações genéricas para o tratamento dos dados pessoais ou; b) ser melhor explicitado o conceito de autorizações genérica. Ou seja, reforça-se a impossibilidade de colher um consentimento específico, razão pela qual essa proibição não deveria existir ou ser melhor delimitada.

Autores da proposta: *MPA, Febraban, Câmara BR, Brasscom* e *ITI.*

(B) O consentimento deverá fazer referência às finalidades informadas.

Autor da proposta: *Febraban.*

Sugestões de redação – Artigo 5º, inciso VII (definição de consentimento)

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] VII – consentimento: toda manifestação inequívoca realizada pelo titular de dados de maneira livre e informada, na qual autorize o tratamento de seus dados pessoais;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] VII - consentimento: é a manifestação livre, inequívoca e informada do titular para o tratamento de seus dados pessoais;

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] VII – consentimento: manifestação ou ação livre e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade;

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] VII – consentimento: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma ou mais finalidades;

Autor da sugestão: *ABDTIC.*

[MODIFICAÇÃO] VII – consentimento: manifestação livre, expressa ou tácita inequívoca, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma ou mais finalidades determinadas;

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] VII - consentimento: toda manifestação inequívoca realizada pelo titular de dados de maneira livre e informada, na qual autorize o tratamento de seus dados pessoais;

Sugestões de redação – Artigo 7º, caput

Autor da sugestão: *Febraban, ESA* e *CNI.*

[MODIFICAÇÃO] Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre e informado do titular, salvo o disposto no art. 11.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11, consoante as determinações da Lei nº8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

4.6.3. Vedação do consentimento como condição para fornecimento de produto ou serviço

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar critérios para aferir se um dado é "indispensável" para o fornecimento de produto ou serviço.

"Estabelecer critérios do que seja 'dados indispensáveis" ao fornecimento de produto ou serviço. Acreditamos ser razoável que o texto apresente critérios para avaliação do que pode ser considerado como dado indispensável, evitando o cenário de incerteza que o texto atual parece criar. Talvez a

própria ideia de indispensabilidade de dados pessoais não seja a via mais adequada para o modelo de consentimento, uma vez que temos dúvidas sobre quais critérios poderiam ser utilizados para se diferenciar um dado dispensável daquele indispensável".

Autores da proposta: *GEPI- FGV.*

(B) A vedação do consentimento como condição para fornecimento de produto ou serviço pode ter efeitos anticoncorrenciais.

"Há possibilidade de que esse dispositivo se enquadre no 1º efeito anticoncorrencial do Guia de Avaliação da Concorrência (por limitar o número de ofertantes), bem como no 2º efeito anticoncorrencial (porque as empresas que já estão no mercado, com grande base de dados formada, terão uma vantagem sobre as novas empresas entrantes, que terão maior dificuldade em prestar serviços gratuitos em troca do acesso aos dados pessoais, na expectativa de formar uma grande base de dados para competir com os operadores históricos)".

Autores da proposta: *SEAE/MF.*

Sugestões de redação – Artigo 7º, § 1º

Autor da sugestão: *Câmara BR* e *Brasscom.*

[MODIFICAÇÃO] § 1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo quando tal fato decorrer da natureza própria do negócio jurídico ou em hipóteses em que os dados forem indispensáveis para a sua realização;

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 1º consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem necessários para a sua realização;

Autor da sugestão: *Câmara BR* e *Brasscom.*

[MODIFICAÇÃO] § 1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo quando tal fato decorrer da natureza própria do negócio jurídico ou em hipóteses em que os dados forem indispensáveis para a sua realização;

Sugestões de redação – Artigo 7º, § 2º

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] § 2º Mesmo em tais hipóteses de indispensabilidade dos dados pessoais para o fornecimento de um produto ou serviço, deve-se assegurar ao titular opções menos invasivas mediante um controle granular dos seus dados pessoais, observando-se, especialmente, os princípios e a proteção contratual disposta nesta legislação.

4.6.4. Qual deve ser a forma para se operacionalizar o consentimento e o controle sobre os dados pessoais?

Nos §3° e 4° do artigo 7°, estabelece-se o modo como seria instrumentalizado o consentimento do titular dos dados pessoais. Os participantes convergem, em sua maioria, para a necessidade de criação de outros mecanismos além da técnica escrita, como de meios digitais e eletrônicos. No entanto, as contribuições rivalizam-se no que diz respeito à preocupação de que tais mecanismos devam empoderar efetivamente o cidadão com o controle sobre seus dados pessoais [*GPoPAI*]; ou se apenas aumentariam a burocracia para o tratamento dos dados pessoais [*Vivo*]. Nessa controvérsia, as propostas dos participantes seguirão uma ordem progressiva – da burocracia ao empoderamento.

Propostas avulsas para a regulação deste tema:

(A) A exigência de cláusulas contratuais destacadas deve ser suprimida.

"É, demasiadamente, onerosa essa obrigação de cláusulas contratuais destacadas, o que aumenta muito a burocracia para o tratamento dos dados pessoais" (Vivo). O consentimento deveria ser, automaticamente, extraído da relação contratual e do uso que se faz dos dados pessoais".

Autores da proposta: *Vivo, SindiTeleBrasil, ITI.*

(B) A obrigação de cláusulas contratuais destacadas deveria incidir apenas para os casos de consentimento expresso, não sendo aplicável para as hipóteses de consentimento implícito.

Essa obrigação deve incidir apenas sobre os casos em que o consentimento expresso é necessário, como seria o caso proposto dos dados sensíveis (vide: subitem A.2 do item 2). Para os casos propostos de consentimento implícito, essa obrigação não deve ser aplicável.

Autores da proposta: *ABRANET, Câmara BR, MPA.*

(C) O consentimento deve ser fornecido por meio de qualquer outra forma – que não somente a escrita –, desde que o seja de maneira inequívoca, como meios

eletrônicos/digitais.

A técnica da escrita não deve ser a única forma para se fornecer o consentimento. É, antiquado (ITI) dar destaque a tal técnica, enquanto que outros meios – informáticos [GSMA], digitais [Claro], caixa de seleção específica nos formulários de cadastro [ABRANET] e por meio de clicks (click agreements) [MPA] – são, também, hábeis para, de forma inequívoca, colher o consentimento do titular dos dados pessoais.

Autores da proposta: *GSMA, Claro, Vivo, MPA, ABRANET, ITI, Febraban, Fiesp, SindiTeleBrasil, CNseg, US Businnes Council.*

(D) As políticas de privacidade devem ser preservadas como a forma adequada para a obtenção do consentimento.

Seguindo a linha de que o consentimento não deveria ser expresso e específico, parte dos participantes entendem que melhor maneira para obter o consentimento do titular dos dados pessoais é continuar apostando nas políticas de privacidade. Elas deveriam: a) estar em local de fácil acesso, desde antes da contratação do serviço (Mariana Cunha e Melo), b) ser de fácil compreensão (Fiesp) para; c) garantir uma informação clara e transparente (Febraban e CNI).

Autores da proposta: *Fiesp (ainda que favorável ao privacy by default como um mecanismo complementar), Febraban e CNI Mariana Cunha e Melo (muito embora, essa participante atente para o fato dos usuários não lerem as políticas de privacidade).*

(E) As políticas de privacidade não são um meio eficaz para a obtenção do consentimento, devendo-se apostar em outras formas.

Há uma série de estudos que comprovam que os usuários não leem os termos de uso. Citando uma série de trabalhos acadêmicos, dentre eles o das pesquisadoras McDonald and Cranor, 2009, os participantes atentam que a relação custo/tempo das políticas de privacidade inviabilizam um controle efetivo dos dados pessoais por meio desse mecanismo. Na verdade, seria surpreende a contínua aposta regulatória de que os usuários se engajem na leitura e compreensão de tais documentos (GEPI-FGV). Por isso, a própria tecnologia deveria empoderar o indivíduo conquanto ao controle das suas informações pessoais (GPoPAI), tal como exemplificado nas subpropostas a seguir

E.1. *Privacy Enhancing Technologies*/PETs (GEPI-FGV, GPoPAI)

O regime jurídico deve oferecer formas simplificadas e/ou dinâmicas para que os cidadãos sejam capazes de escolher que informações estão dispostos a fornecer às empresas pelos produtos e serviços (GEPI-FGV). É a ideia da adoção de tecnologias que empoderem o cidadão com um melhor controle de suas informações pessoais - *privacy enhancing Technologies* (GPoPAI). Os proponentes trazem inúmeros exemplos, dentre os quais:

a) o *tracking preferences* da W3C que possibilita que o usuário pré-estabelecer as suas opções de privacidade para que tal protocolo, automaticamente, externalize-as durante a sua navegação. Essa tecnologia seria capaz, assim, de "massificar" as preferências de privacidade do consumidor diante, igualmente, de uma grande gama de relações por ele travadas em que o fluxo de seus dados pessoais é contínuo (GPoPAI);

b) *Terms of Service; Didn't Read* que consiste na avaliação e classificação de políticas de privacidade e termos de uso em uma escala de conceitos de A à E. Busca-se informar o usuário a partir de critérios padronizados de avaliação, sem que para isso ele tenha ler as respectivas

políticas de privacidade (GEPI-FGV).

A ideia dos participantes é, portanto, que haja um catálogo em aberto para que essas novas tecnologias possam operacionalizar, efetivamente, o consentimento, o que não tem ocorrido com a prática corrente dos termos de uso e políticas de privacidade.

E.2. *Privacy by default* (Fiesp, GPoPAI, e CTS-FGV)

A própria configuração dos serviços e produtos deve contribuir para que o titular dos dados pessoais exerça um melhor controle sobre as suas informações pessoais. Por padrão (privacy by default), os serviços e produtos devem ter configurações menos invasivas e mais protetivas à privacidade. Assim, os usuários não precisariam tomar qualquer medida afirmativa para proteger seus dados pessoais, facilitando-se o seu controle. Por exemplo, os dados pessoais não devem estar acessíveis a um número indefinido de indivíduos para haver, justamente, um controle mais robusto (CTS-FGV).

Autores da proposta: *GEPI-FGV, GPoPAI, CTS-FGV, Fiesp (outros participantes trazem a mesma linha argumentativa, mas não a conectam com essa solução proposta por esses participantes).*

(F) A lei deve deixar clara o ônus que o responsável do tratamento tem na produção de prova sobre o consentimento.

"A fusão do parágrafo 3° com o parágrafo 8°, já que ambos dispõem sobre o ônus que o responsável pelo tratamento tem com relação a prova do consentimento".

Autores da proposta: *Câmara BR, Brasscom, ABINEE* e *ABRANET.*

(G) A lei deve adotar a terminologia "comprovação", pois utilizar o verbo "certificar" pode causar confusão com meios digitais de certificação.

Sugere-se a substituição da palavra certifique pela palavra comprove, pois a palavra "certifique", presente no texto do anteprojeto, transmite a ideia de "certificação", o que pode ser confundido com os meios digitais de certificação.

Autores da proposta: *Febraban.*

Sugestões de redação:

Autor da sugestão: *CTS-FGV.*

[MODIFICAÇÃO] Art. 6º [...] princípio da privacidade por padrão, pelo qual as configurações de privacidade dos produtos ou serviços devem ser as mais protetivas possíveis, considerando os estritos fins que legitimaram a coleta de dados, tanto em aspectos técnicos como organizacionais, sendo facultado ao usuário alterá-las para padrões mais públicos.

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] §4º Quando necessário, o consentimento expresso deverá ser fornecido de

forma destacada das demais cláusulas contratuais.

Autor da sugestão: *Claro.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por escrito ou por qualquer outro meio em direito admitido.

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido de forma inequívoca, por qualquer meio que o identifique.

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por escrito, deverá ser constatado tacitamente a partir da ação ou inação do titular dos dados pessoais ou por outro meio que o demonstre, por exemplo requerendo ao usuário para clicar em um comando contendo a declaração de que ele está ciente e compreendeu todos os termos e condições.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por qualquer meio que comprove a manifestação de vontade do titular.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique, inclusive eletrônico/digital.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique, exceto quando o tratamento dos dados pessoais for condição indispensável para o fornecimento do produto ou serviço ou para o exercício de direito.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO E INCLUSÃO] § 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.

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] § 3º O consentimento deve ser obtido através de qualquer método adequado onde os indivíduos estejam cientes que estão fornecendo seu consentimento para o tratamento de dados pessoais. Caso o consentimento do titular dos dados deva ser dado após um pedido eletrônico, tal pedido deve ser claro, conciso e não desnecessariamente confuso para o uso do serviço para o qual eles são fornecidos.

Autor da sugestão: *ABINEE.*

[MODIFICAÇÃO] § 3º O consentimento deve ser fornecido por qualquer meio nos termos da legislação vigente.

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] §3º O consentimento deve ser fornecido por qualquer meio, cabendo ao responsável pelo tratamento dos dados pessoais a prova do consentimento.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 3º O consentimento deverá ser fornecido por qualquer meio, cabendo ao responsável pelo tratamento dos dados pessoais a prova do consentimento ou por qualquer meio que o certifique.

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais, podendo ser disposto no corpo do contrato, salvo nos casos em que o consentimento puder ser tacitamente constatado a partir de ação ou inação do usuário.

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] § 5º O operador tem o dever de informar o titular a respeito do tratamento dos seus dados pessoais, utilizando-se das técnicas adequadas para que ele exerça um controle significativo sobre seus dados, como, por exemplo, um processo contínuo de interação pelo qual haja um consentimento recorrente e renovado, visando, todavia, não sobrecarregá-lo com o exercício de tal direito;

§ 6º O quanto disposto no parágrafo anterior não prejudica a adoção de outras tecnologias que, concomitantemente, empoderem o titular com um controle significativo sobre seus dados pessoais, tal como a implementação de mecanismos que expressem, de forma automatizada, as suas preferências de privacidade no tocante ao fluxo de seus dados pessoais.

§ 8º Os produtos e serviços deverão implementar mecanismos que assegurem, por configuração padrão, somente o tratamento de dados pessoais que são, realmente, necessários para o propósito específico que ensejou a coleta e que não vão além do mínimo necessário para tanto, bem como, por padrão, evitar o acesso por um número indefinido de indivíduos (*redação atribuída de acordo com a modernização da diretiva da União Europeia*).

4.6.4. Comentários sobre a revogação do consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei deve explicitar que a revogação do consentimento não pode prejudicar direitos de terceiros de boa-fé.

Autor da proposta: *SindiTeleBrasil.*

(B) A lei deve criar um dever de disponibilização de canal de fácil acesso para a revogação do consentimento.

"Deve ser disponibilizado canal de fácil acesso que viabilize a revogação do consentimento. Além de revogável a qualquer tempo, deve, também, ser obrigatório disponibilizar um canal facilmente acessível para melhor operacionalizá-la, evitando que o objetivo do parágrafo seja frustrado pelo processo".

Autor da proposta: *Daniel Astone.*

(C) A lei deve criar a obrigação de emissão de protocolo comprobatório da revogação de consentimento.

"Após a revogação do consentimento, deve haver a emissão de documento comprovando o ato. Deveria ser obrigatório o fornecimento de um protocolo, confirmando-se a desautorização para o tratamento dos dados pessoais".

Autores da proposta: *Flávio Costa.*

(D) A revogação do consentimento deve ser realizada por escrito e por meio da autorização do titular.

Autores da proposta: *ABDTIC.*

(E) A lei deve estabelecer que o procedimento de revogação do consentimento deva ser gratuito.

Autores da proposta: *ABRANET.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] § 6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular, mas este poderá perder a gratuidade de alguns serviços;

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] § 6º O consentimento pode ser revogado a qualquer momento, podendo haver ônus para o titular nos casos em que os dados objeto do consentimento sejam indispensáveis à regular prestação do serviço, de modo que o usuário poderá ser alertado sobre a possibilidade de haver interrupção ou perda do serviço;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] § 6º O titular dos dados terá o direito de retirar seu consentimento a qualquer tempo, mediante leis aplicáveis e acordos contratuais (sem prejuízo às leis existentes). A retirada do consentimento não afetará a legalidade do tratamento baseado no consentimento antes de sua retirada ou a exigência legal de reter dados históricos. Quaisquer outros benefícios ou serviços ao titular que dependerem deste consentimento ou o tratamento ou retenção de dados pode ser imediatamente interrompido mediante o processamento da solicitação;

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente concedido e a manutenção pelo responsável da informação que não possa ser retirada do banco de dados, conforme os termos do Artigo 11, inciso;

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular, desde que sua revogação não implique na impossibilidade de cumprimento das obrigações do contrato, hipóteses nas quais a revogação do consentimento importará na rescisão do contrato com a imposição dos ônus da rescisão em desfavor do titular dos dados;

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] § 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;

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular, ressalvados sempre os direitos de terceiros de boa-fé;

Autor da sugestão: ABDTIC.

[MODIFICAÇÃO] §6º O consentimento pode ser revogado a qualquer momento, por escrito e

mediante confirmação do titular, sem ônus adicional para este.

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] §6º O consentimento pode ser revogado a qualquer momento, por procedimento gratuito.

4.6.5. Sugestões de novas definições e deveres relacionados ao consentimento

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais, respeitando as provisões do art. 10, §2 no caso de alteração das finalidades.

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] O operador tem o dever de informar o titular a respeito do tratamento dos seus dados pessoais, utilizando-se das técnicas adequadas para que ele exerça um controle significativo sobre seus dados, como, por exemplo, um processo contínuo de interação pelo qual haja um consentimento recorrente e renovado, visando, todavia, não sobrecarregá-lo com o exercício de tal direito.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

CAPÍTULO II – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I – ~~Consentimento~~ Requisitos para o tratamento

Art.~~.~~ 7º O tratamento de dados pessoais somente ~~é permitido após~~ poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento pelo titular de consentimento livre~~, expresso, específico~~ e ~~informado do titular, salvo o disposto no art~~ inequívoco;

II – ~~11~~ para o cumprimento de uma obrigação legal pelo responsável;

III – pela administração pública, ~~§ 1º O consentimento~~ para o tratamento e uso compartilhado de dados ~~pessoais não pode ser condição~~ relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos;

IV – para ~~o fornecimento~~ a realização de ~~produto~~ pesquisa histórica, científica ou ~~serviço~~ estatística, garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de ~~direito, salvo em hipóteses~~ direitos em ~~que os dados forem indispensáveis~~ processo judicial ou administrativo;

VII – para a ~~sua realização~~ proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII – para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX – quando necessário para atender aos interesses legítimos do responsável, respeitados os interesses ou os direitos e liberdades fundamentais do titular.

§ 1º Nos casos de aplicação do disposto nos incisos II e III, o titular deverá ser informado do tratamento de seus dados.

§ 2º ~~É vedado~~ No caso de descumprimento do disposto no § 1º, o operador ou o responsável pelo tratamento de dados ~~pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação~~ poderá ser responsabilizado.

§ 3º O ~~consentimento deverá ser fornecido por escrito ou por outro meio que o certifique. § 4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais. § 5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o~~ tratamento de dados pessoais~~. § 6º O consentimento pode~~ cujo acesso é público deve ser ~~revogado a qualquer momento, sem ônus para o titular. § 7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis~~ realizado de acordo com esta lei, considerando a ~~boa-fé ou~~ finalidade, a ~~equidade. § 8º Cabe ao responsável~~ boa-fé e o ~~ônus da prova de~~

interesse público que ~~o consentimento do titular foi obtido em conformidade com o disposto nesta Lei~~ justificou a sua disponibilização.

4.7. Consentimento de menores de idade para o tratamento de seus dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 8º 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.

Neste artigo, discute-se a faixa etária dos titulares que serão tratados pela lei de forma mais protetiva. Isso significa que para tratar dados de titulares dessa faixa etária não bastará obter o consentimento (ainda que esse seja ainda necessário); em função da imposição legal, também será necessário que o tratamento de dados seja compatível com a "condição peculiar de pessoa em desenvolvimento" do titular.

É possível observar que as propostas de alteração nesse dispositivo têm escopos diversos. Muitos se preocuparam em igualar a faixa etária protetiva traçada pelo anteprojeto com o regramento acerca da incapacidade civil disposto no código civil. Além desse grupo de participantes, alguns outros buscaram abordar a questão da revogação do consentimento por pais e responsáveis legais.

Propostas avulsas para a regulação deste tema:

(A) A lei deve utilizar a faixa etária de "capacidade relativa" civil, não criar outra.

Autores da proposta: *Bruna de Rosa, Keity Mary Kjhelin Teixeira Vieira, Náthaly Morgani, Gabriela Martins, Elis, Rodrigo Junqueira, Amanda Arrivabene, Gabriele Ferreira, Kilcy Bispo, Wagner Silveira, Raissa Guimarães, Elizane Gomes Felipe de Ivanoff, Jhonata Goulart Serafim, Aparecida Cristina, Fiesp e CNseg.*

(B) A lei deve definir claramente que indivíduos com 18 anos completos não estão cobertos por proteção especial conferida a crianças e adolescentes.

"Sugere-se a inclusão da palavra 'incompletos' depois da expressão '18 anos' de forma que indivíduos

com 18 anos já completados não sejam alvo da norma protetiva, à semelhança do que acontece no código civil".

Autores da proposta: *Vivo.*

(C) A lei deve estabelecer que pais e responsáveis devem se autenticar para estar aptos a revogar o consentimento do titular com idade entre 12 e18 anos.

Autores da proposta: *ITI.*

(D) A lei não deve ter um regime especial para o consentimento dado por menores de idade.

"Sugerimos excluir esta seção porque existe um direito geral de retirar o consentimento que cobriria situações relativas a titulares dos dados de todas as idades. Além disso, a conformidade com esta exigência demandaria a coleta de informações adicionais significativas de todos os usuários com idades entre doze e dezoito, contrariando a meta geral de minimizar a coleta de dados pessoais".

Autores da proposta: *US Business Council.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 8º. O titular de dados pessoais com idade inferior a dezoito anos somente poderá fornecer consentimento para tratamento de dados pessoais a que refere esta lei, em conformidade com o que dispõe a Lei Federal nº 10.406, de 10 de janeiro de 2002 (Código Civil).

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 8.º O titular de dados pessoais com idade entre doze e dezoito anos incompletos, 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.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos poderá fornecer consentimento para tratamento de seus dados pessoais, tratamento esse que deve respeitar a sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 8º 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.~~

4.7. Hipótese de fornecimento de consentimento de menores de idade por pais ou responsáveis legais

REDAÇÃO LEVADA A DEBATE

Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.

Tal como no artigo anterior, a discussão neste artigo toma duas vertentes: de um lado há aqueles participantes que requerem que o anteprojeto iguale o tratamento dispensado pelo Código Civil aos absolutamente incapazes e, de outro, há aqueles que têm preocupações de ordem mais prática e apontam dificuldades de identificar os indivíduos e, consequentemente, de saber suas idades na rede.

Propostas avulsas para a regulação deste tema:

(A) O responsável pelo tratamento de dados pessoais não deve ter um dever específico de "respeitar a condição peculiar" de menor de idade.

"Não deve haver restrição ao tratamento dos dados pessoais oferecidos baseada na condição peculiar do menor de 12 anos.

Entendemos que 'respeitar a condição peculiar' de menor de idade, como 'pessoa em desenvolvimento', não deve ser um dever do responsável pelo tratamento de dados. Se o consentimento deve ser fornecido pelos pais, é deles a decisão de escolher qual o conteúdo adequado, como parte do controle dos pais.

Sugerimos a remoção deste artigo ou a alteração segundo nossa proposta de redação".

Autores da proposta: *ABRANET e Câmara BR.*

(B) Os pais devem fornecer o consentimento para o tratamento de dados de menores de idade até 16 anos.

É necessário alinhar o artigo com o disposto no Código Civil sobre capacidade civil do indivíduo, aumentando a idade para 16.

Autores da proposta: *Gabriela Martins, Fiesp* e *TV Aberta.*

(C) A lei deve especificar de que modo os pais ou responsáveis legais podem fornecer o consentimento para o tratamento de dados pessoais dos menores de 12 anos.

O artigo é ineficaz, pois uma vez que pelo meio digital existe uma grande dificuldade de se comprovar a real identidade do indivíduo em questão, qualquer um em posse dos dados dos pais ou responsáveis legais (inclusive a própria criança) pode garantir a autorização deste tratamento de dados do menor.

Esta medida só serve para eximir de culpa o órgão responsável pelo tratamento dos dados, uma vez que terá este respaldo legal para afirmar que a autorização foi garantida pelos pais. Crianças menores de 16 anos deveriam ficar totalmente excluídas do fornecimento de dados em ambiente online, diminuindo assim os riscos de fraude [*Amanda*]. Não vejo uma condição de operacionalização do presente artigo no ambiente virtual. Talvez este artigo deve contar com incisos que especifiquem um modo diferenciado de consentimento capaz de atender uma efetiva proteção das crianças [*Lucas Zolet*].

Autores da proposta: *Amanda Arrivabene e Lucas Zolet.*

Sugestões de redação:

Autor da sugestão: *ABRANET e Câmara BR.*

[MODIFICAÇÃO] Art. 9º - No caso do titular de dados pessoais de até doze anos de idade, o consentimento deverá ser dado pelos pais ou responsáveis legais.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento dos seus dados respeitar sua condição peculiar de pessoa em desenvolvimento.

Após a compilação das contribuições a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi suprimido conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.~~

4.8. Elementos necessários para o fornecimento do consentimento para tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:

I – finalidade específica do tratamento;

II – forma e duração do tratamento;

III – identificação do responsável;

IV – informações de contato do responsável;

V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita a:

a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;

b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e

c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.

§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.

§ 2º Em caso de alteração de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.

§ 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.

4.8.1. Informações ao titular de dados pessoais para obtenção do consentimento

No caput do artigo 10º podemos identificar grande preocupação de alguns participantes com a forma como o titular deve ser informado sobre o tratamento de dados. Segundo eles, impor que o titular seja informado de "forma clara, adequada e ostensiva" acaba por gerar inseguranças, na medida em que não há diretrizes de como respeitar tal imposição.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve elencar adjetivos genéricos ("forma clara, adequada e ostensiva") como requisito para obtenção do consentimento para coleta e tratamento de dados pessoais.

"É importante determinar o que significa 'de forma clara, adequada e ostensiva' para o legislador para que as empresas possam cumprir com essa obrigação. Sugerimos a retirada desse trecho ou uma maior especificação do mesmo". [*Câmara BR*]

"As palavras 'clara, adequada e ostensiva' podem ser demais amplas e descoladas dos objetivos da lei, criando um cenário de insegurança jurídica". [*Cisco*]

Autores da proposta: *Câmara BR* e *Cisco.*

(B) A lei deve especificar como deve ser cumprido o dever de informar o titular de dados pessoais no momento da obtenção do consentimento.

"Propomos nova redação tendo em vista evitar confusões acerca dos modos de informar o consentimento. Isso porque há artigos que requerem o estabelecimento de comunicação entre a plataforma de aplicações e o usuário em certas situações, como as descritas nos parágrafos 3° e 4° do Art. 10.

Não se deve entender que, diante dessas situações, não seja possível informar o consentimento em formato eletrônico de click wrap agreement*, daí a necessidade de, ao menos exemplificativamente, inserir na redação essa possibilidade".*

Autores da proposta: *MPA.*

(C) A lei deve incluir um dever para que os termos de uso e políticas de privacidade sejam redigidos de maneira clara e simplificada.

"Sugerimos a inclusão do dever de os termos de uso serem redigidos de maneira clara e simplificada. Temos dúvida quanto à efetividade das disposições constantes do art. 10 para garantir que de fato a informação será dada ao cidadão de forma satisfatória, de modo a habilitá-lo a se decidir ou não pelo consentimento. Isto porque, como é público e notório, são raros os casos em que as pessoas de fato leem os termos de uso, redigidos em geral de forma muito técnica, sem destaques e muito longos, o que desincentiva o usuário a se informar extensamente".

Autores da proposta: *Proteste.*

(D) A lei deve criar um regime especial para casos em que dados possam ser manipulados posteriormente.

"O artigo deve levar em consideração diferentes formas de manipulação de dados incompatíveis com suas disposições, tal como os mecanismos de busca. A manipulação dos dados nem sempre decorre de um contrato.

*É o caso de mecanismos de busca como o Google. Qual a sua situação, nesse caso? Não há aval prévio quanto às informações que serão fornecidas. Torna-se, assim, imprescindível esclarecer se mecanismos de buscas e instrumentos afins estão cobertos pela legislação e, em caso afirmativo, como artigos como o 10º se enquadrariam nas obrigações desses '*edge providers*". A aplicação integral do art. 10º, por exemplo, inviabiliza a atividade desses mecanismos de busca no Brasil".*

Autor da proposta: *Roberto Taufick.*

4.8.2. Dever de informar a finalidade específica do tratamento de dados pessoais

Neste inciso todas as sugestões se voltaram ao termo "finalidade específica". Segundo os participantes deveria haver certa flexibilidade para que os responsáveis pelo tratamento determinassem suas finalidades ao longo do tempo.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve prever que um dever de informar "finalidade específica", mas apenas de informar "finalidades".

"Sugerimos a retirada do termo "específica" do inciso. Em muitos casos, não é possível prever todas as finalidades específicas do tratamento de dados previstos no inciso I. Sugere-se, assim, a alteração

na redação mencionando apenas "finalidades".

Autores da proposta: *ABRANET, Brasscom, Câmara BR, MPA, Febraban e ITI.*

(B) A lei deve prever que o consentimento possa ser dado para mais de uma finalidade.

Autores da proposta: *SindiTeleBrasil.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] I – finalidades específicas do tratamento;

4.8.3. Dever de informar a forma e a duração do tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei não deve trazer um dever de informar a "forma" do tratamento de dados pessoais.

"Forma" de tratamento deve ser suprimida do inciso. As finalidades e a duração já seriam informações suficientes para possibilitar ao usuário tomar a decisão pelo consentimento ou não. A inclusão da forma é burocratizar demasiadamente o processo [*Claro* e *SindiTeleBrasil*]

"*Sugere-se a retirada do termo 'forma'. Isso porque a forma como esse tratamento será realizado é decisão que cabe ao responsável, que considerará seus recursos e meios disponíveis. Além disso, com a rápida evolução da tecnologia, haverá a possibilidade do surgimento de novas foras de tratamento que, no entanto, não serão previstas no momento do consentimento*" [*Febraban*].

Autores da proposta: *Claro, Febraban* e *SindiTeleBrasil.*

(B) A lei deve criar uma exceção ao dever de informar "forma" e "duração" do tratamento de dados pessoais para fins de pesquisas de mercado.

"Pesquisas de Mercado devem ser isentas da obrigação de informar o usuário sobre a (I) forma e (II) duração do tratamento de dados, deverão somente informar o usuário de que a coleta de dados é referente a uma Pesquisa de Mercado. Isso porque os dados coletados para a pesquisa de mercado (I) nunca serão disponibilizados de forma individualizada para terceiros e (II) poderão ser usados sem limitação no tempo, já que estes continuam válidos até que uma mudança social relevante os torne obsoleto".

Autores da proposta: *ABEP.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] II – duração do tratamento;

Autor da sugestão: *ABEP.*

[MODIFICAÇÃO] II – forma e duração do tratamento ou sobre o fato de se destinar a Pesquisa de Mercado, o que dispensa as informações deste item;

4.8.4. Dever de informar dados de contato do responsável pelo tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever um dever de informação do contato do encarregado definido pelo responsável pelo tratamento de dados pessoais.

Autores da proposta: *SindiTeleBrasil.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] IV – informações para contato com o encarregado do responsável;

4.8.5. Dever de informar os sujeitos ou categorias de sujeitos que podem ter contato com os dados pessoais do titular

Propostas avulsas para a regulação deste tema:

(A) A lei não deve criar um dever de informar os sujeitos ou categorias de sujeitos que podem ter contato com os dados pessoais do titular.

Autor da proposta: *Claro.*

(B) A lei deve criar apenas um dever de informar as categorias de sujeitos, não sujeitos individualmente.

"Sugerimos que seja obrigatório informar o titular apenas com relação às categorias de sujeitos, e não os sujeitos propriamente. Nossa sugestão faz sentido em um ambiente comercial em que as parcerias estão constantemente se alterando.

Medidas como as propostas neste inciso do anteprojeto acabam por aumentar os custos transacionais das empresas (podendo até inviabilizar operações) e não são adequadas para proteger os consumidores. Uma forma mais viável de compatibilização dos direitos em questão seria a opção legislativa pelo opt out.

*Outra alternativa seria a adoção do "*soft opt in*" em que o consentimento restaria comprovado diante da continuidade da relação comercial entre titular e responsável pelo tratamento".*

Autores da proposta: *ABEMD.*

(C) A lei deve restringir o dever de informar os sujeitos e categorias de sujeitos que terão contato com os dados pessoais do titular a uma estimativa.

"A mudança da redação se justifica diante da inviabilidade prática da aplicação do dispositivo tal como disposto no anteprojeto. Isso porque é difícil dizer antecipadamente quais serão todos os terceiros, ou todas as categorias de terceiros, para quem os dados poderão ser comunicados, no todo ou em parte, da mesma forma em relação ao âmbito de difusão".

Autores da proposta: *MPA.*

Sugestões de redação:

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] V- sujeitos ou as categorias estimadas de sujeitos para os quais os dados podem ser comunicados, bem como a estimativa de âmbito de difusão;

4.8.6. Dever de informar as responsabilidades dos agentes que realizarão o tratamento de dados

Propostas avulsas para a regulação deste tema:

(A) A lei deve especificar quais são as informações acerca das obrigações dos agentes que devem ser informadas ao titular dos dados pessoais.

Autores da proposta: *MPA.*

Sugestões de redação:

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] VI – responsabilidades, nos termos desta lei, dos agentes que realizarão o tratamento;

4.8.7. Dever de informar os direitos do titular: a possibilidade de acesso e retificação dos dados e de revogação do consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei deve deixar claro que os direitos do titular referem-se somente a dados pessoais.

"Sugerimos o acréscimo da palavra "pessoais" para especificar que os dados que podem ser acessados, retificados e ter o consentimento revogado são apenas os dados pessoais".

Autores da proposta: *Bruno Diego, Brasscom, Câmara BR* e *ABRANET.*

(B) A lei deve conter o dever de informar que a revogação do consentimento pode implicar no cancelamento do serviço oferecido.

Autor da proposta: *Bruno Diego, Cisco* e *ABRANET*.

4.8.8. Dever de informar os direitos do titular: nulidade do consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever a possibilidade de indenização por danos e prejuízos resultantes do consentimento enganoso.

Segundo os participantes que defenderam esta proposta, deveria ser inserido no corpo da norma a expressão "sem prejuízo das sanções de natureza civil e penal cabíveis" ou algo semelhante, para assegurar o direito das pessoas que foram enganadas, bem como dar maior efetividade ao dispositivo lega.

Autores da proposta: *Gabriela Martins, Rafaela 16 e Gleison.*

(B) O consentimento enganoso deveria ser "anulável", não "nulo".

"O consentimento enganoso deveria ser anulável, e não nulo. O ideal é que a redação preveja que tais dados são anuláveis, não nulos, já que a interpretação sobre a forma de apresentação do pedido de consentimento dependeria de uma série de questões que deveriam ser melhor definidas".

Autores da proposta: *ABDTIC.*

4.8.9. Dever de informar os direitos do titular: casos de obtenção de novo consentimento

Propostas avulsas para a regulação deste tema:

(A) O responsável apenas deveria obter novo consentimento em caso de alteração significativa das informações referidas.

Autores da proposta: *US Business Council, Câmara BR* e *ITI.*

(B) A lei deve substituir o dever de obtenção de novo consentimento pela comunicação dos titulares, quando informações que lhe devem ser informadas forem alteradas.

"Frente ao direito do titular de requisitar o término do tratamento, a simples comunicação dos usuários em função de alteração de informação parece suficiente para proteger o titular. Além disso, no caso de mantida a necessidade de um novo consentimento, o anteprojeto deveria estipular qual seria o procedimento específico a ser adotado, o que não está previsto". (MPA)

Autores da proposta: *GSMA, MPA* e *SindiTeleBrasil.*

(C) A lei não deve criar obrigação de obtenção de um novo consentimento, caso apenas informações de contato do responsável pelo tratamento de dados pessoais forem alteradas.

"Sugere-se a retirada do inciso III da redação do parágrafo. Isso porque há informações que não necessariamente são relevantes para o titular e, portanto, não ensejam novo consentimento. Estas informações devem ser meramente informadas aos usuários".

Autores da proposta: *Febraban.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 2º Em caso de alteração de informação referida nos incisos I, II ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] § 2º Em caso de alteração de relevante natureza de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após

destacar de forma específica o teor das alterações.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 2º Em caso de alteração de informação referida nos incisos I, II ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

4.8.10. Novos deveres de comunicação de informações ao titular de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) O titular de dados pessoais deve ser apenas comunicado, caso as informações de contato do responsável pelo tratamento de dados pessoais forem alteradas.

Sugere-se a inclusão do inciso III da redação do parágrafo. A alteração indicada é necessária, pois a identificação do responsável está diretamente ligada as suas informações de contato, por este motivos devem ser fornecidas em conjunto ao titular. Esta sugestão é combinada com a exposta acima, de retirar a obrigatoriedade de novo consentimento em casos de alteração de informações de contato do responsável.

Autores da proposta: *Febraban.*

(B) O dever de informar as informações de contato atualizadas do responsável pelo tratamento de dados pessoais deve se efetivar por sítio eletrônico.

Autores da proposta: *CNseg.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 3º Em caso de alteração das informações constantes nos incisos III e IV do caput, o responsável deverá comunicar ao titular as informações atualizadas.

Autor da sugestão: *CNseg.*

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

4.8.11. Dever de informar o titular de dados pessoais continuamente

Propostas avulsas para a regulação deste tema:

(A) Deve ser determinada uma periodicidade segundo a qual o usuário será informado sobre a continuidade do tratamento de dados de sua titularidade.

"Além disso, é necessário cautela para que a repetição de avisos não façam om que usuários deixem passem a desconsiderá-los. O texto do anteprojeto não determina a periodicidade dos avisos, diante disso, sugerimos que a periodicidade seja de 1 ano".

Autor da proposta: *Fiesp.*

(B) Os princípios da transparência e da finalidade suprem a necessidade de informar continuamente o usuário.

Autor da proposta: *SindiTeleBrasil.*

(C) No caso de coleta continuada, a obrigação de informar o titular regularmente apenas deveria incidir na hipótese de alteração no tempo de coleta dos dados.

Autor da proposta: *US Business Council.*

(D) O dever de informar o titular de dados pessoais sobre tratamento contínuo deve ser compatibilizado com a existência de mecanismos que permitem a coleta de dados em intervalos regulares e com o risco de fadiga na comunicação por excesso de avisos.

Autor da proposta: *ITI.*

(E) A lei não deve prever dever de informar continuamente o titular de dados pessoais.

"*Sugerimos a supressão deste parágrafo. A necessidade de informar o titular de fatos dos quais ele já tem consciência se mostra um fardo excessivo para as empresas e até mesmo para os usuários. Neste caso, disponibilizar as informações atualizadas e a política de privacidade parecem um caminho mais efetivo*".

Autor da proposta: *MPA.*

(F) A lei deve excetuar a atividade de pesquisa de mercado do dever de informar continuamente o titular de dados pessoais.

"*Quando se tratar de coleta para fins de pesquisa de mercado, será desnecessário informar o titular de forma contínua, bastando o primeiro consentimento no momento inicial da coleta. Os dados coletados para a pesquisa de mercado (I) nunca serão disponibilizados de forma individualizada para terceiros e (II) poderão ser usados sem limitação no tempo, já que estes continuam válidos até que uma mudança social relevante os torne obsoletos*".

Autores da proposta: *ABEP.*

Sugestões de redação:

Autor da sugestão: *ABEP.*

[MODIFICAÇÃO] § 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, sendo desnecessária a informação sempre que a coleta se destine a Pesquisa de Mercado, desde que esse fato tenha sido informado no momento da coleta.

Autor da sugestão: US Business Council.

[MODIFICAÇÃO] § 4º Nas atividades que importem em coleta continuada de dados pessoais, além do período determinado, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 4º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado dessa condição no momento de emissão do seu consentimento.

4.8.12. Previsão de encerramento da relação contratual, caso haja revogação do consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever expressamente o término da relação contratual ou de serviço, caso haja revogação do consentimento.

Acreditamos ser necessário deixar disposto na lei que essa revogação pode acarretar em término do serviço porque a indústria pode não ter como prosseguir com sua atividade sem a anuência do titular. Nesse caso, com a revogação, o titular não poderá cobrar da empresa a continuidade dos serviços.

Autores da proposta: *Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[INCLUSÃO] § 5º A revogação do consentimento conforme alínea b pode resultar no término da

relação contratual ou de serviço.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 8º 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.~~

~~Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo~~ deverá ter acesso facilitado às informações sobre o tratamento ~~respeitar sua condição peculiar~~ de ~~pessoa em desenvolvimento.~~

~~Art. 10º No momento do fornecimento do consentimento~~ seus dados, ~~o titular será informado~~ que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre ~~os seguintes elementos:~~, entre outros:

I – finalidade específica do tratamento;

II – forma e duração do tratamento;

III – identificação do responsável;

IV – informações de contato do responsável;

V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita a:

a) possibilidade de ~~não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;~~

~~b) possibilidade de~~ acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; ~~e~~

~~c)~~ b) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta ~~Lei~~ Lei; e

c) possibilidade de não fornecer o consentimento, na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências da negativa.

§ 1º ~~Considera-se nulo~~ Na hipótese em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva.

§ 2º Em caso de alteração de informação referida ~~nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.~~

~~§ 3º Em caso de alteração de informação referida~~ no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.

~~§ 4º~~ 3º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado ~~regularmente~~ periodicamente sobre ~~a continuidade~~ as principais características do tratamento, nos termos definidos pelo órgão competente.

§ 4º Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados. § 5º O órgão competente poderá dispor sobre os meios referidos no parágrafo anterior.

4.9. Hipóteses de dispensa do consentimento

REDAÇÃO LEVADA A DEBATE

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:

I – cumprimento de uma obrigação legal pelo responsável;

II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;

IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

V – exercício regular de direitos em processo judicial ou administrativo;

VI – proteção da vida ou da incolumidade física do titular ou de terceiro;

VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

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

§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.

§ 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

4.9.1. Dados anonimizados como hipótese de dispensa do consentimento para o tratamento

Sugestões de redação:
Autor da sugestão: *Claro (essa sugestão não veio acompanhada de justificativa).* **[INCLUSÃO]** § 4 º O tratamento de dados anônimos ou anonimizados;
Autor da sugestão: *Câmara BR (essa sugestão não venha acompanhado de justificativa).* **[INCLUSÃO]** § 4º O tratamento de dados anônimos ou de dados pessoais que tenham passado por processo de dissociação independe de consentimento, exceto no caso de dado reidentificado, que terá o tratamento de dado pessoal, nos termos desta lei;

4.9.2. Deve haver a definição de "dados de acesso público irrestrito"? Qual deve ser ela?

Segundo o texto posto para debate pela Secretaria Nacional do Consumidor, o consentimento é a regra geral para legitimar o tratamento dos dados pessoais, determinando (i) legalidade de toda e qualquer atividade de processamento de dados pessoais. Há, no entanto, uma série de exceções à essa regra, dentre as quais a exceção para "dados de acesso público irrestrito" – artigo 11, caput.

Nesse contexto, houve uma série de contribuições que apontaram para a necessidade de se criar uma definição de dados de acesso público restrito, sob pena da criação de uma série de incertezas em torno da sua aplicação: "*Se os dados pessoais tiverem sido disponibilizados em redes sociais pelos próprios titulares, eles seriam considerados dados privados de acesso público? Eles estariam sujeitos à proteção estabelecida nessa lei?"* [*ABDTIC*].

Houve, assim, um certo consenso de que se deveria explicitar um conceito para dados de acesso público irrestrito. Contudo, o debate público trouxe controvérsias sobre qual deveria ser a extensão dessa definição, a fim de delimitar o próprio alcance da hipótese de dispensa do consentimento a ela relacionada. A sistematização dessas contribuições procurou seguir uma lógica progressiva daquelas que pretendem restringir mais o conceito de dados de acesso público irrestrito e, por conseguinte, essa hipótese de dispensa do consentimento.

Propostas avulsas para definições de "dados de acesso público irrestrito" organizadas da menos para a mais restritiva.

(A) Dado que esteja disponível à consulta pública gratuita, por obrigação legal ou por livre divulgação pelo próprio titular, por qualquer meio, ao público.

Autores da proposta: *CNseg e ABRANET*.

(B) Dado que seja manifestamente público ou dados que o seu titular tenha tornado públicos por sua própria iniciativa.

Por essa conceituação, dados que constam de listas telefônicas de acesso público estariam contemplados por essa exceção, como, por exemplo, o nome, endereço, CEP, telefone fixo do titular dos dados.

Autores da proposta: *SindiTeleBrasil e Vivo.*

(C) Dado que façam parte de bases de dados públicas de acesso geral.

Autor da proposta: *Câmara BR*.

(D) Bancos de dados públicos.

Autor da proposta: *US Business Council.*

(E) Essa definição deveria ser contextual a ser determinada pela autoridade de garantia de proteção de dados pessoais.

Isto porque, poderá ser o caso de tais dados serem sensíveis, o que demandaria uma análise contextual dessa exceção a ser balizada pela autoridade de proteção de dados pessoais.

Autora da proposta: *Joana Varon*.

(F) O uso dos dados pessoais de acesso público restrito não deve permitir o seu cruzamento com outra base de dados pessoais.

Essa proibição justificar-se-ia pelo fato de haver a possibilidade de haver o cruzamento com dados sensíveis.

Autor da proposta: *Rodrigo Veleda.*

(G) Essa dispensa do consentimento deveria respeitar as demais obrigações previstas na lei, especialmente o princípio da finalidade.

Assim, não poderia o dado ser tratado para uma finalidade incompatível com aquela para a qual o fora inicialmente. Um dos defensores dessa tese argumenta que essa finalidade deve ser vista de acordo com o motivo pelo qual o dado pessoal foi publicizado. Desta forma, impedir-se-ia que tais dados pessoais fossem comercializados, evitando-se que empresas centralizassem tais informações para a criação perfis e categorização dos cidadãos.

Autores da proposta: *ITS-Rio e Paulo C.A*.

(H) Somente quando os dados vierem a público por opção do seu titular.

Muitas vezes, essa publicidade pode se dar de maneira irrestrita, mas não por vontade do seu titular, o que seria, extremamente, problemático quando se tem vista que dados sensíveis poderiam ser enquadrados nessa categoria. Conclui, assim, por uma abordagem restritiva dessa exceção.

Autores da proposta: *Veridiana/Intervozes.*

Sugestões de redação:

Autor da sugestão: *CNseg* e *ABRANET.*

[INCLUSÃO] 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;

Autor da sugestão: *SindiTeleBrasil* e *Vivo.*

[INCLUSÃO] VI - dados de acesso público irrestrito: são dados pessoais dos titulares que sejam manifestamente públicos, ou dados que o seu titular tenha tornado públicos por sua própria iniciativa;

Autor da sugestão: *Câmara BR.*

[INCLUSÃO] XVI – dados pessoais de acesso público irrestrito: são aqueles dados que fazem parte de bases de dados públicas de acesso geral;

Autor da sugestão: *Veridiana/Intervozes.*

[MODIFICAÇÃO] II – sem fornecimento de consentimento do titular, quando os dados tenham sido disponibilizados por ele de maneira pública e irrestrita, ou nas hipóteses em que for indispensável para:

4.9.2. As exceções à regra do consentimento devem ser ampliadas ou restringidas?

Questão central e diretamente prejudicial à regra estabelecida de que os cidadãos devem consentir para o fluxo de seus dados pessoais são, justamente, os casos em que seria excepcionada tal regra. Nesse contexto, o embate travado no debate público foi controverso com relação ao alargamento ou encolhimento de tal artigo, tal como com respeito de novas exceções a serem criadas com uma maior ou menor restrição.

O mapeamento do debate público visa a captar essa polarização do debate, tendo sido dada uma atenção especial em reportar uma nova hipótese de dispensa para o consentimento: a existência de interesses legítimos. Em que pese ter havido certa convergência para a sua implementação, os participantes debateram intensamente a forma pela qual esta nova exceção seria absorvida, verificando-se, que, qualitativamente, essas sugestões são controversas entre si.

Respostas controversas coletadas na plataforma de debate:

(A) Deve ser ampliado para prever...

A.1. ...uma nova hipótese para interesses legítimos (consentimento implícito ou tácito) (*ITI, Centre for Information Policy Leadership, GSMA, Fiesp, IAB, ABDTIC, ABINEE, ABRANET, BSA, Sky, US*

Business Council e CNseg, Febraban, RELX Group, Cisco, Brasscom, Câmara BR, Claro e Vivo)[20]

> Seguindo a lógica do argumento de que o consentimento do titular dos dados pessoais não deve ser sempre expresso, deve haver a previsão da hipótese de dispensa do consentimento para interesses legítimos para abrir caminho à hipótese de consentimento tácito/implícito [*ITI*]. Tal como ocorre na diretiva da União Europeia (Diretiva 95\46\CE, em seu artigo 7º, alínea f), essa nova exceção à regra do consentimento assegurará a possibilidade da realização de tratamento de dados de forma facilitada em situações nas quais não haveriam impactos indevidos sobre o indivíduo e seus direitos. Ao final, os titulares dos dados pessoais não seriam onerados com a necessidade de manifestação de seu consentimento a cada instante [*IAB*]. Isso otimizaria o controle dos dados pessoais, evitando-se a fadiga do consumidor [*Centre for Information Policy Leadership e ITI, Câmara BR*].

A.2. ...uma nova hipótese para Big Data; (*GSMA)*

> Tal como já acontece com pesquisas científicas, jornalísticas e históricas no APL, também deve haver uma exceção para uso de Big Data. Isso porque, tal tecnologia vale-se da técnica da anonimização dos dados, o que reduz, significativamente, eventuais danos da atividade. O APL deve, portanto, fomentar o uso da anonimização e para isso a própria tecnologia do Big data.

A.3. ...uma nova hipótese para interesses públicos; *(RELX Group, Centre for Information Policy Leadership e MPA)*

> O consentimento também não deve ser obrigatório quando o tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados [Centre for Information Policy Leadership]. Essa exceção está, aliás, alinhada com a Lei de Acesso à Informação (Lei nº 12.527/2011), que elimina a necessidade de consentimento em diversas circunstâncias, inclusive "à proteção do interesse público e geral preponderante" (Artigo 31, V). Sem essa nova exceção, não seriam permitidas, por exemplo, o tratamento de dados para a prevenção à fraudes e até investigações criminais. Por fim, tal exceção está em consonância com a Diretiva de Proteção de Dados da EU. Isso poderia alcançar, até mesmo, a proteção da propriedade intelectual, reprimindo dentre outras atividades ilegais.

A.4. ...uma nova hipótese para internet das coisas; (*Brasscom)*

> O tratamento de dados realizados entre dispositivos M2M (máquina à máquina) deveriam dispensar a necessidade de consentimento, na medida em inviabilizariam o desenvolvimento de Internet das Coisas no Brasil. A regulamentação nesse momento pode retardar o desenvolvimento dessas tecnologias em um período de crise financeira, quando elas poderiam ser mais necessárias. Sendo assim, propõe-se que os dispositivos caracterizados como Internet das Coisas não devam se submeter à regra geral do consentimento.

A.5. ...uma nova hipótese para quando os dados forem provenientes de órgãos reguladores ou jurídicos; *(RELX Group)*

> Os dados provenientes de órgãos reguladores ou jurídicos devem ser excluídos das várias instâncias mencionadas no APL, dentre as quais da regra geral da necessidade do consentimento do titular dos dados pessoais para seu tratamento.

A.6. ...uma nova hipótese com relação ao cadastro negativo de crédito dos consumidores;

20 Nota: apesar de alguns proponentes observar que essa nova exceção deveria seguir um teste de ponderação com os direitos do titular dos dados pessoais, verificou-se que as sugestões de redação de dispositivos não enunciaram qual seria esse teste. Por isso, tais contribuições foram alocadas nesse campo ampliativo de novas exceções ao consentimento.

(Febraban)

> Deve haver uma nova exceção de consentimento com relação ao cadastramento de consumidores no cadastro negativo de crédito. Isso porque, requerer o consentimento por parte do consumidor para tal prática acabaria por inviabilizá-la. A informação a respeito do inadimplemento é uma informação preciosa às instituições financeiras e às entidades que concedem venda a prazo, pois elas são norteadoras da análise de risco de crédito e evitam o superendividamento do consumidor. Assim, deve haver um diálogo com o quanto já disposto no Código de Defesa do Consumidor que prevê o envio, apenas, de uma comunicação prévia quando da ocasião da abertura dos registros de consumo.

A.7. ...uma nova hipótese para o cumprimento de uma obrigação infralegal [inciso I]; *(CNseg)*

> Merece revisão a hipótese de dispensa de consentimento apenas para o 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. Assim, a dispensa do consentimento deveria contemplar não apenas o cumprimento de obrigação legal, mas, também, um dever imposto (infralegal) por uma a autoridade fiscalizadora/órgão regulador do setor.

A.8. ...que a hipótese para o cumprimento de uma obrigação legal autorize o uso dos dados para a prevenção de fraudes e incidentes de segurança, o que poderá ser terceirizado [inciso I]; *(ITI)*

> O cumprimento de uma obrigação legal deve autorizar o responsável pelo tratamento dos dados pessoais a melhorar a segurança e prevenir fraudes. Em tais situações, o responsável poderia, ainda, contratar um terceiro para executar tais tarefas. Em tais casos, o consentimento do titular dos dados pessoais deveria ser excepcionado.

A.9. ...que a hipótese para fins de pesquisas estatísticas seja substituída por pesquisas de mercado, ampliando-a [inciso IV]; *(ABEP)*

> Este inciso deve excluir no seu rol as pesquisas estatísticas, substituindo-a pelo termo "pesquisas de mercado". Dessa forma, tornar-se-á mais clara a exceção estabelecida à regra do consentimento, alcançando um escopo maior.

A.10. ...que a dissociação dos pessoais não seja uma exigência para hipótese de pesquisas históricas, científicas e estatísticas [inciso IV]; *(Câmara BR)*

> A dissociação dos dados pessoais não é compatível com a natureza dos tipos de informações de pesquisa histórica, científica ou estatística. Por tal razão, tal obrigação deveria ser suprimida da lei.

A.11. ...que a hipótese de dispensa para fins de pesquisas históricas, científicas e estatísticas seja ampliada para fins jornalísticos, genealógicos, artísticos, culturais, acadêmicos, estatística, artísticos, literários ou de interesse público [inciso IV]; *(Associação da Liberdade Religiosa e Negócios)*

> Com o objetivo de proteger o interesse público, preservando-se a memória da coletividade, os registros históricos e, por fim, permitindo-se os avanços acadêmicos e científicos, o inciso IV deve ser expandido para incluir mais hipóteses de dispensa de consentimento. Por exemplo, a legislação canadense permite, em seu parágrafo 7(c), a coleta de dados sem consentimento ou conhecimento do titular para fins jornalísticos, artísticos ou literários. A legislação europeia, em seu artigo 8(d), permite que fundações, associações e organizações mantenham informações sensíveis, sem o consentimento explícito e específico, do seu titular.

A.12. ...para que a hipótese relativa à proteção da vida ou incolumidade física alcance, também, a

pessoa do responsável pelo tratamento dos dados pessoais [inciso VI]; *(ITI)*

> Este inciso também deve abarcar a proteção da vida ou da incolumidade física do responsável e, não, somente, de terceiros e do titular dos dados pessoais.

(B) Deve ser restringido para...

B.1. ... que haja um teste de razoabilidade/ponderação para limitá-la, no caso de uma nova hipótese de interesses legítimos *(ITS-Rio e GPoPAI)*

> A grande preocupação com advento da nova exceção por interesses legítimos é que tal exceção sabote, ou mesmo, fragilize o pilar normativo do APL, qual seja, o consentimento como a regra geral para o tratamento dos dados pessoais [*GPoPAI*]. Por isso, os proponentes que debateram, controversamente, acerca dessa nova exceção acabam por sugerir que a lei preveja, expressamente, um teste para a ponderação dos interesses envolvidos que deve levar em conta uma série de fatores [*ITS-Rio*]. Os fatores de tal teste pretendem delimitar a aplicabilidade de tal exceção, bem como impor obrigações ao responsável pelo tratamento de dados pessoais para que seja preservada a privacidade dos cidadãos. Dentre algumas obrigações, está prevista, por exemplo, a prática de anonimização dos dados pessoais, minimizando-se, sempre que possível, os riscos para a privacidade do titular dos dados pessoais. Essa exceção baseada no interesse legítimo deve ser estar atrelada mais uma desqualificação do consentimento como sendo expresso, e, por tal razão, tal teste visa assegurar uma esfera de controle mínima por parte do titular dos dados pessoais [*GPoPAI*].

B.2. ...suprimir a hipótese com relação ao compartilhamento de dados para o exercício de direitos ou deveres em leis ou regulamentos da administração pública [inciso II] *(Felipe de Ivanoff, Lucas Zolet, ABRANET, Câmara BR – esse último participante sugere, inclusive, que o artigo seja revisto completamente, pois exclui a necessidade de consentimento para quase todas as atividades da administração pública)*

> Esta hipótese de dispensa do consentimento é uma porta escancarada para que a administração pública tenha mecanismos de vigilância exagerados e discricionários. Tal como está, o direito à privacidade será, facilmente, violado. O tratamento de dados pessoais sem o consentimento do titular deveria ocorrer somente mediante decisão judicial [*Felipe*].

B.3. ...delimitar a hipótese com relação ao compartilhamento de dados para o exercício de direitos ou deveres em leis ou regulamentos da administração pública, exigindo-se um dever de anonimização e a observância de todos os princípios previstos na lei [inciso II] *(Joana Varon, Luiz Perin Filho, Proteste e Veridiana/Intervozes, GPoPAI – embora esse último sugerido um capítulo próprio para o tratamento de dados pessoais no setor público, que impõe outras limitações)*

> Trata-se de uma exceção ao consentimento muito ampla. Ela deve, explicitamente, sujeitar-se a todos os princípios elencados no artigo 6° desta lei, bem como prever a anonimização de dados, sempre que possível ou compatível com a finalidade da utilização do dado [*Joana*]. Ainda que para as atividades da administração pública e realização de políticas públicas seja muitas vezes necessário o tratamento de dados sem consentimento específico do seu titular. Os riscos de mau uso que podem se desdobrar dessa compreensão inicial devem ser minimizados mediante tais mecanismos de controle [*Veridiana/Intervozes*].

B.4. ...que a hipótese com relação ao compartilhamento de dados para o exercício de direitos ou deveres em leis ou regulamentos da administração pública, submeta-se aos princípios da necessidade do APL e da eficiência da administração pública [inciso II] *(GPoPAI – embora tenha sugerido um capítulo próprio para o tratamento de dados pessoais no setor público que impõe outras limitações)*

> Essa previsão é, extremamente, genérica, devendo-se vincular aos princípios da necessidade

do APL e da eficiência da administração pública. Isso, em tese, restringiria essa hipótese que, da forma como está redigida, é extremamente permissiva ao Estado.

B.5. ...suprimir a hipótese com relação ao cumprimento de obrigações contratuais ou pré-contratuais [inciso III]; (*GPoPAI, Proteste e Veridiana/Intervozes)*

Seja para um procedimento pré-contratual, seja para o cumprimento de obrigações contratuais, o titular deve, durante as tratativas negociais ou no próprio contrato, autorizar o tratamento de seus dados pessoais [GPoPAI]. Por exemplo, um consumidor que esteja solicitando crédito a uma instituição financeira deve ser informado sobre quais dados seus serão coletados e como serão analisados por tal instituição durante a avaliação da concessão ou não do crédito. Munido dessas informações, ele tem o direito de decidir se autoriza esses procedimentos de maneira a dar ou não continuidade à solicitação de crédito [Veridiana/Intervozes]. Dito de outra forma, não há nenhuma justificativa para que o consentimento seja dispensado na fase pré-contratual. É importante que o cidadão ou consumidor estejam cientes de que nesta fase seus dados serão analisados, a fim de que autorize ou não o tratamento e possa, também, decidir se quer ou não dar continuidade ao processo de contratação. [Proteste].

B.6. ...suprimir a hipótese relativa a pesquisas [inciso IV]; *(TV Aberta)*

Caso essa hipótese permaneça, haverá uma margem muito grande para que todo tipo de coleta de dados ocorra sob o pretexto da exceção para a realização de pesquisas científicas, históricas ou estatísticas.

B.7. ...exigir que na hipótese relativa a pesquisas históricas, científicas e estatísticas não haja identificação dos titulares dos dados pessoais, bem como exigir que informações que permitam tal atribuição sejam armazenadas em separado [inciso IV]; *(CTS-FGV)*

Tal hipótese deve ser mais restrita. Tal como nas discussões da Comissão Europeia para a reforma do marco de proteção de dados pessoais, deve-se determinar que os dados pessoais podem ser tratados para fins de pesquisas históricas, estatísticas e científicas desde que: (i) não possam ser realizadas sem o processamento de dados que não permitam a identificação do titular e (ii) sempre que possível para tais fins, os dados que permitam a atribuição de informações a um titular identificado ou identificável sejam mantidos/armazenados em separado de outras informações.

B.8. ...limitar a hipótese relativa a pesquisas históricas, científicas e estatísticas para os casos de pesquisa "pura" [inciso IV]; *(GPoPAI, Daniel Astone e Giovanna Carloni)*

Tal hipótese deve estar restrita, literalmente, aos casos de pesquisa "pura", desvinculando-a de interesses comerciais e políticos. Isso implica, por exemplo, a completa vedação de pesquisas voltadas a atividades de inteligência e investigação criminal, dado o potencial danoso em face da liberdade do cidadão.

B.9. ...limitar a hipótese relativa a pesquisas realizadas somente por órgãos públicos [inciso IV]; *(Tagwato)*

Tal hipótese deveria se restringir a pesquisas somente realizadas por órgão público. Caso contrário, a dissociação ou o consentimento expresso deverão ser obrigatórios.

B.10. ...limitar que a hipótese relativa ao exercício regular de direitos seja proveniente de um processo judicial ou autorização por lei, substituindo-se o termo processo administrativo [inciso V]; *(Claro)*

Deve haver a exclusão do termo "administrativo", substituindo-o pelo termo "ou quando permitido em lei". Assim, por exemplo, somente será admitida a quebra de sigilo em processo

judicial e, por conseguinte, com ordem judicial. Caso contrário, haveria situações em que, por exemplo, autoridades policiais e entes administrativos requereriam informações sem ordem judicial.

B.11. ...suprimir a hipótese relativa à proteção da vida ou da incolumidade física do titular ou de terceiro [inciso VI]; *(ABRANET, Gabriela Martins e TV Aberta)*

Essa hipótese dá margem à realização de atividades de vigilância pelo Estado, devendo ser suprimida. A saúde não pode servir como um pretexto para uma violação da intimidade de modo tão genérico.

B.12. ...que a hipótese relativa ao compartilhamento de dados para a proteção da vida ou da incolumidade física submeta-se aos princípios da necessidade do APL e da eficiência da administração pública [inciso VI]. *(GPoPAI – embora tenha sugerido um capítulo próprio para o tratamento de dados pessoais no setor público que impõe outras limitações)*

Essa previsão é, extremamente, genérica, devendo-se vincular aos princípios da necessidade do APL e da eficiência da administração pública. Isso, em tese, restringiria essa hipótese que, da forma como está redigida, é extremamente permissiva ao Estado.

Sugestões de redação para ampliar exceções ao consentimento:

Autor da sugestão: *GSMA.*

[INCLUSÃO] VIII – prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular;

Autor da sugestão: *IAB.*

[INCLUSÃO] VIII – a persecução de interesses legítimos do responsável, desde que o tratamento seja feito de acordo com os princípios desta Lei e sejam preservados os direitos e garantias do titular;

Autor da sugestão: *Febraban.*

[INCLUSÃO] VIII – cumprimento de uma obrigação legal ou execução de atividade legítima pelo responsável;

Autor da sugestão: *RELX Group.*

[INCLUSÃO] IX – o tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º;

Autor da sugestão: *Centre for Information Policy Leadership.*

[INCLUSÃO] VIII – processar os dados de forma compatível com um interesse legítimo do responsável ou de um terceiro, desde que esses interesses não sejam anulados por danos ou impacto negativo sobre o titular de dados;

Autor da sugestão: *Câmara BR.*

[INCLUSÃO] VIII – a persecução de interesses legítimos e legais do responsável, desde que o tratamento seja feito de acordo com os princípios desta Lei e sejam preservados os direitos e garantias do titular;

Autor da sugestão: *Brasscom.*

[INCLUSÃO] VIII - legitimo interesse do responsável;;

Autor da sugestão: *Claro.*

[INCLUSÃO] VIII - atender a interesse legítimo do responsável pelo tratamento de dados ou terceiros a quem os dados forem comunicados;

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] VIII – prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados;

Autor da sugestão: *RELX Group.*

[INCLUSÃO] VIII - o tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

Autor da sugestão: *Centre for Information Policy Leadership.*

[INCLUSÃO] IX - O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

Autor da sugestão: *MPA.*

[INCLUSÃO] VIII – a proteção de direitos de Propriedade Intelectual, seja por meio de ordem judicial ou não;

IX – proteção de direitos, evitando fraude e atividades ilegais;

X – garantir o cumprimento de termos de uso e cláusulas contratuais.

Autor da sugestão: *Brasscom.*

[INCLUSÃO] IX -realizado nos serviços entre dispositivos M2M (máquina a máquina);

Autor da sugestão: *RELX Group.*

[MODIFICAÇÃO] Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando os dados são provenientes de órgãos reguladores ou jurídicos, ou quanto ao tratamento for indispensável para:

Autor da sugestão: *Febraban.*

[INCLUSÃO] O funcionamento de bancos de dados e cadastros de consumidores, com informações a respeito do inadimplemento de obrigações por parte do cadastrado, que seguirão as regras do art. 43 da Lei 8.078/90 – Código de Defesa do Consumidor.

Autor da sugestão: *CNseg.*

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

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] V – realização de pesquisa histórica, científica ou estatística, garantida a dissociação dos dados sensíveis;.

Autor da sugestão: *Associação da Liberdade Religiosa e Negócios.*

[MODIFICAÇÃO] IV – realização de pesquisa histórica, genealógica, artística, científica, cultural ou acadêmica, estatística ou de interesse público, garantidas as medidas de segurança aplicáveis;

Sugestões de redação para restringir exceções ao consentimento:

Autor da sugestão: *ITS-Rio.*

[MODIFICAÇÃO] Tratamento necessário ao atendimento de interesses legítimos do responsável pelo tratamento, desde que não prevaleçam interesses e direitos do titular do dado, considerando-se a natureza e a fonte do interesse legítimo, a existência de um interesse público relevante a autorizar o tratamento e o impacto nos direitos dos titulares dos dados.

Porém, referido dispositivo deve estabelecer, de forma expressa, que a ponderação dos interesses

envolvidos deve levar em conta os seguintes fatores:

• A natureza e a fonte do interesse legítimo e se o tratamento de dados e necessário para o exercício de direitos fundamentais ou se é feito no interesse público ou, ainda, se seus benefícios recebem reconhecimento da sociedade;

• O impacto nos direitos do titular dos dados e quais seriam as suas legítimas expectativas com relação ao que será feito com os seus dados, além da natureza dos dados tratados - se sensíveis ou não - e como serão tratados;

• As medidas adotadas pelo responsável pelo tratamento para minimizar o impacto na privacidade do titular dos dados, sejam tecnológicas, em termos de políticas de privacidade ou mesmo de transparência.

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito, bem como nas seguintes hipóteses:

VIII - quando os dados pessoais forem objeto de procedimento de anonimização lastreado em padrão de razoabilidade mínimo a ser definido, periodicamente, e fiscalizado pelo órgão competente, de modo a mitigar o processo de reversibilidade da anonimização, devendo estar referido procedimento restrito às seguintes hipóteses e requisitos:

a) no setor público para a implementação de políticas públicas;

b) no setor privado, o tratamento dos dados anonimizados deverá observar o contexto da relação com o operador, em seu deu previamente a coleta dos dados pessoais, e as expectativas legítimas do seu titular, como dispõe o princípio da adequação nos termos do inciso II do artigo 6;

c) a reversão do processo de anonimização é vedado, salvo mediante consentimento dos próprios titulares dos dados pessoais;

d) o compartilhamento e o uso de base de dados anonimizadas deve ser objeto de publicidade, seja pelo setor privado ou pelo setor público, de acordo, respectivamente, como o §3 do artigo 39, e §1 do artigo 6, informando-se, em todos os casos, o órgão competente a seu respeito;

e) a disponibilização pública parcial e/ou completa de uma base de dados anonimizadas estará sujeita à autorização do órgão competente, o qual avaliará os riscos de sua re-identificação, possibilitando-se, sempre que possível, a publicação de estatísticas agregadas ou outro formato adequado para fins de se prevenir a reversão do processo de anonimização.

VIII - para interesses legítimos do operador, desde que não se sobreponha aos direitos fundamentais, liberdade e privacidade do titular previsto no artigo 1º, levando-se em consideração:

a) a relação entre o propósito especificado, originariamente, para a coleta dos dados pessoais e o tratamento adicional a que se refere esse inciso;

b) o contexto da relação com o operador, em que se deu previamente a coleta dos dados pessoais, e as expectativas legítimas do seu titular, de acordo com o disposto no inciso II do artigo 6º;

c) a natureza dos dados pessoais e o impacto que o tratamento dos dados pessoais terá sobre o

titular;

d) a adoção de medidas de segurança capazes de prevenis a ocorrência de danos em virtude do tratamento dos dados pessoais, e, sempre que possível, a anonimização, de acordo o que dispõem, respectivamente, os artigos 6º, inciso VIII, e as obrigações estabelecidas no inciso VII deste artigo 11.

Autor da sugestão: *Joana Varon.*

[MODIFICAÇÃO] II – tratamento e uso compartilhado dos dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública, com a anonimização dos dados pessoais sempre que possível;

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] II – tratamento de uso compartilhado de dados para o atendimento eficiente das finalidades próprias do Estado, observando-se o quanto disposto no artigo 24 e seguintes;

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] III – realização de pesquisa histórica, científica ou estatística, desde que tais atividades não estejam vinculadas a atividade comercial, de administração pública, investigação criminal ou inteligência, garantindo-se, sempre que possível, a anonimização dos dados pessoais;

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] VI – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, observando-se o quanto disposto no artigo 24 e seguintes;

4.9.3. Dever de tratamento exclusivo para as finalidades e por menor tempo possível nos casos de dispensa do consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei não deve estabelecer um dever de tratamento pelo "menor tempo possível", e sim que a limitação temporal esteja relacionada aos propósitos específicos da coleta.

Autores da proposta: *MPA.*

(B) O dever de tratamento exclusivo para as finalidades também deve ser obrigação no tratamento de dados públicos de acesso irrestrito.

"*Lei deve deixar claro que, apesar do fato de que o tratamento de dados públicos de acesso irrestrito dispensa consentimento, o responsável pelo tratamento deverá observar os demais ditames previstos na futura lei, em especial o princípio da finalidade, não podendo o dado ser tratado para uma*

finalidade incompatível com aquela para a qual o dado foi tratado inicialmente".

Autores da proposta: *ITS-Rio.*

(C) A lei deve criar uma exceção ao dever de tratamento "pelo menor tempo possível" a contratos de serviço "por tempo indeterminado".

"Excluir os contratos por tempo indeterminado do dever de tratar os dados dentro do menor período de tempo possível. 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 recomendável, para afastar qualquer dúvida, incluir uma ressalva expressa a esses tipos de contratos".

Autores da proposta: *CNseg.*

(D) A lei deve estabelecer um prazo máximo para o tratamento, ao invés de utilizar o menor período de tempo possível como parâmetro.

Autores da proposta: *ABDTIC.*

(E) A lei deve utilizar a terminologia "período legítimo", ao invés do parâmetro do "menor tempo possível".

"Utilizar "período legítimo" como parâmetro no lugar de "o menor período de tempo". Pois o período legítimo nem sempre será o menor possível".

Autores da proposta: *ABRANET.*

Sugestões de redação:

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] § 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas, pelo período de tempo legitimamente necessário, conforme os princípios gerais dispostos nesta Lei e garantidos os direitos do titular.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] § 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.

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] § 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e por um período razoável de tempo, de acordo com o objetivo específico da coleta.

4.9.4. Responsabilização em caso de descumprimento de dever de informação do titular em casos de dispensa do consentimento para cumprimento de dever legal

Neste parágrafo, a dúvida dos participantes gira em torno da falta de indicação de como a responsabilização dos agentes de tratamento será feita, ou seja, no caso de descumprimento do dever, como serão encontrados os responsáveis e aplicadas as sanções.

Propostas avulsas para a regulação deste tema:

(A) A modalidade da responsabilização pelo descumprimento do dever de informação deve ser especificada.

Autores da proposta: *CNseg*[21]*, Anderson, TV Aberta, Jéssica Brasil, ITI e Fiesp.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 3º No caso de descumprimento do disposto no §2°, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado administrativa, civil e penalmente, nos termos desta Lei e da legislação em vigor.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] § 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.

Autor da sugestão: *SindTeleBrasil.*

[MODIFICAÇÃO] § 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados será responsabilizado;

[21] O *CNseg* propõe a aplicação das sanções previstas no art. 50 do texto levado à debate.

4.9.5. Obrigações e exceções adicionais nas hipóteses de dispensa do consentimento

Sugestões de redação:
Autor da sugestão: *Câmara BR.* **[INCLUSÃO]** § 4º O tratamento de dados anônimos ou de dados pessoais que tenham passado por processo de dissociação independe de consentimento, exceto no caso de dado reidentificado, que terá o tratamento de dado pessoal, nos termos desta lei.
Autor da sugestão: *ABEP.* **[INCLUSÃO]** §2º No caso das empresas de pesquisa de mercado, o tratamento dos dados pessoais poderá ser realizado por tempo indeterminado desde que garantida a confidencialidade dos dados;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~11.~~ **9º** O consentimento ~~será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:~~

~~**I – cumprimento de uma obrigação legal pelo responsável;**~~

~~**II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;**~~

~~**III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto**~~ previsto no ~~§ 1º do~~ art. ~~6º;~~

~~**IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;**~~

~~**V – exercício regular de direitos em processo judicial ou administrativo;**~~

~~**VI – proteção da vida ou da incolumidade física do titular ou de terceiro;**~~

~~**VII – tutela da saúde.**~~ **7º**, ~~com procedimento realizado~~ I deverá ser livre e inequívoco e fornecido por ~~profissionais da área da saúde~~ escrito ou por ~~entidades sanitárias~~ qualquer outro meio que o certifique.

§ 1º ~~Nas hipóteses de dispensa de~~ Caso o consentimento seja fornecido por escrito, ~~os dados devem~~ este deverá ser ~~tratados exclusivamente para as finalidades previstas e pelo menor período~~ fornecido em cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao responsável o ônus da prova de ~~tempo possível, conforme os princípios gerais dispostos~~ que o consentimento foi obtido em conformidade com o disposto nesta Lei

§ 3º É vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.

§ 4º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§ 5º O consentimento pode ser revogado a qualquer momento, ~~garantidos os direitos~~ mediante manifestação expressa do titular.

§ ~~2º Nos casos~~ **6º** Em caso de ~~aplicação do disposto~~ alteração de informação referida nos incisos I ~~e II~~, ~~será dada publicidade a esses casos~~ II, ~~nos termos do parágrafo 1º~~ III ou V do art. 8º, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 7º O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais, respeitados os direitos e liberdades fundamentais do titular, devendo ser necessário e baseado em uma situação concreta.

§ 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, II.

§ ~~3º No caso de descumprimento do disposto no §2o, o operador ou o~~ **2º** O responsável ~~pelo~~ deverá adotar medidas para garantir a transparência do tratamento de dados ~~poderá~~ baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

§ 3º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser ~~responsabilizado~~ anonimizados sempre que compatível com a finalidade do tratamento.

§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo.

4.10. Dados pessoais sensíveis

REDAÇÃO LEVADA A DEBATE

Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:

I – com fornecimento de consentimento especial pelo titular:

a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e

b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou

II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para:

a) cumprimento de uma obrigação legal pelo responsável;

b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

d) exercício regular de direitos em processo judicial ou administrativo;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

§ 1º O disposto neste artigo aplica-se a qualquer tratamento capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º Nos casos de aplicação do disposto nos itens 'a' e 'b' pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do §1º do art. 6º.

4.10.1. Propostas gerais sobre tratamento de dados sensíveis

Vários dos comentários no caput do artigo 12 demandavam uma definição mais objetiva de dados pessoais sensíveis. Segundo os participantes, critérios objetivos para a definição seriam capazes de diminuir a incerteza e as inúmeras interpretações sobre o conceito e, com isso, reforçariam a proteção dos titulares de dados.

Nesse sentido, é importante ressaltar a contribuição da participante Mariana Cunha e Melo, a qual buscou trazer elementos objetivos para a análise dos dados sensíveis:

Propostas avulsas para a regulação deste tema:

(A) Dados sensíveis seriam melhor tratados por legislação específica.

"O risco da previsão genérica do projeto de lei é sua aplicação a dados sensíveis em qualquer contexto, não apenas naqueles em que eles de fato mereçam proteção especial. Isso porque dados sensíveis não devem ser definidos tão somente pelo seu conteúdo, mas também pelo contexto em que esses dados são divulgados, ou seja, a mesma informação pode ser mais ou menos sensível a depender do contexto em que ela é divulgada.

A sensibilidade da informação deve ser sempre aliada a um contexto específico, em que o indivíduo espere um resguardo especial do dado".

Autores da proposta: *Mariana Cunha e Melo.*

(B) A lei deve permitir o tratamento de dados sensíveis com determinadas finalidades.

Seriam elas: "*(i) qualidade do serviço; (ii) segurança e prevenção contra fraude; (iii) solução de problemas e correções de falhas; e (iv) aperfeiçoamentos em geral do produto / serviço*"

Autor da proposta: *ITI.*

4.10.2. Como deve ser dado o consentimento para tratamento de dados sensíveis?

O debate trouxe muita discussão acerca do significado de consentimento especial. *ABDTIC* e *ITI*, por exemplo, argumentaram que o conceito não estava claro, enquanto a participante

Febraban demandou que o inciso fizesse menção expressa às alíneas *a* e *b*, de forma que o caráter "especial" do consentimento ficasse mais claro.

Aparte dessa discussão, outros participantes opinavam acerca de formas de autorização do tratamento de dados sensíveis. Foi possível distinguir duas opiniões opostas na plataforma: a primeira delas buscando criar maior facilidade para o oferecimento do consentimento; e a segunda, preferindo revestir a autorização de mais requisitos formais.

Respostas controversas coletadas na plataforma de debate:

(A) Através de consentimento expresso.

"Acreditamos que o consentimento para o tratamento de dados sensíveis deve ser expresso, enquanto o consentimento para outros tipos de tratamento deve ser inequívoco".

Quem defendeu isso? *Câmara BR, Brasscom e ABRANET*.

(B) Através de consentimento expresso colhido através de um procedimento formal específico.

O consentimento deve ser expresso, através notificação pessoal do cidadão através de carta registrada, exigindo-se o retorno de documento firmado concordando com os termos do uso dos dados. Renovando-se o ato a cada nova oportunidade de utilização dos dados.

Quem defendeu isso? *TV Aberta + Merchant = Peculato e adamir.*

Propostas avulsas para a regulação deste tema:

(A) A lei não deve exigir dois níveis de consentimento para o tratamento de dados sensíveis.

Autores da proposta: *ITI.*

(A) A lei não deve prever obrigação de alertar o titular do dado quanto aos riscos envolvidos no tratamento de dados sensíveis.

"*Tal como está, a redação do artigo pode gerar confusão ao invés de beneficiar os titulares. Isso porque não há - além da discriminação que já é vedada- riscos existentes no tratamento de dados sensíveis que não estejam presentes também no tratamento de dados pessoais comuns"*.

Autores da proposta: *CNseg.*

Sugestões de redação:

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] Artigo 11, inciso I, b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados;

4.10.3. Exceções da regra de consentimento especial para dados sensíveis para a administração pública ou para o caso de dados de acesso público irrestrito

Propostas avulsas para a regulação deste tema:

(A) A lei deve restringir a exceção ao consentimento para dados de acesso público irrestrito apenas para os dados que o titular optar por tornar públicos.

Autora da proposta: *Veridiana/Intervozes.*

(B) A lei deve prever que em casos de exceção à regra do consentimento o titular deve ser informado, salvo casos de segurança nacional e guarda de soberania.

Autor da proposta: *decko.*

(C) Dados de acesso público irrestrito devem incluir dados provenientes de órgãos reguladores ou jurídicos, como o Poder Judiciário.

Autor da proposta: *RELX Group.*

(D) A lei deve criar um dever de anonimização de dados sensíveis quando tratados no âmbito da administração pública.

"*Entendemos que, de fato, nem sempre há a possibilidade de obter de consentimento específico do titular na ocasião do tratamento de dados já coletados no âmbito da administração pública. Os riscos de mau uso que decorrem dessa impossibilidade de consentimento devem, no entanto, ser minimizados".*

Autores da proposta: *Veridiana/Intervozes.*

(G) A lei não deve prever que a exceção de uso compartilhado de dados sensíveis pela administração pública possa ser prevista em decreto.

"Deve ser suprimida do texto a exceção para uso compartilhado de dados pela administração pública em razão de deveres previstos em decreto. Isso porque os decretos não passam pela intensa deliberação democrática inerente às leis. Excluída essa exceção, os titulares terão maior proteção".

Autores da proposta: *Lucas Zolet.*

Sugestões de redação:

Autor da sugestão: *Veridiana/Intervozes.*

[MODIFICAÇÃO] Artigo 11, inciso II – sem fornecimento de consentimento do titular, quando os dados tenham sido disponibilizados por ele de maneira pública e irrestrita, ou nas hipóteses em que for indispensável para;

(...) b) tratamento e uso compartilhado dos dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública, com a anonimização dos dados pessoais sempre que possível;

Autor da sugestão: *RELX Group.*

[MODIFICAÇÃO] II - sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito ou quando os dados são provenientes de órgãos reguladores ou jurídicos...;

4.10.4. Exceção à regra de consentimento especial para dados sensíveis para realização de pesquisas

Neste ponto, com exceção da contribuição da *ABEP* (que será tratada mais abaixo), todas as contribuições buscaram encontrar formas de aumentar a restrição com relação a hipótese de dispensa de consentimento da alínea c. Inclusive, alguns participantes argumentaram que a realização deste tipo de pesquisa nem deveria ser uma hipótese de dispensa, sendo, portanto, adequado e necessário requisitar consentimento para esses casos.

Propostas avulsas para a regulação deste tema:

(A).A lei deve ser mais restrita quanto à exceção da regra de consentimento especial para dados sensíveis para a realização de pesquisas.

"Esse dispositivo deve ser mais restrito. Pode-se, por exemplo, determinar que somente é possível utilizar dados de pessoas já falecidas".

Autora da proposta: *Gabriela Martins.*

(B) A lei deve prever mecanismos de controle (como aprovação em conselho de ética acadêmica) para casos de exceção da regra de consentimento especial para dados sensíveis para a realização de pesquisas.

"Deve haver maior restrição, neste sentido propõe-se que somente pesquisas aprovadas por conselho de ética de instituições reconhecidas pelo MEC sejam autorizadas a realizar o tratamento de dados

sensíveis sem necessidade de consentimento".

Autores da proposta: *Prof. Marcos e Névoa.*

(C) A lei deve obrigar o consentimento prévio em casos de pesquisas.

"A abertura para fins de pesquisas estatística dá margem para que pesquisas quantitativas que subsidiem ações comerciais sejam feitas sem conhecimento do titular.

Mesmo no caso das duas outras exceções (pesquisas históricas e científicas) não há porque não se considerar o consentimento prévio do titular de dados. Lembrando sempre que, dados meramente estatísticos podem ser coletados sem passar por essa, em se tratando de dados anônimos". [*Daniel Astone*]

"Sempre que a pesquisa tratar de dados não anonimizados deverá haver consentimento do titular. Isso não é só benéfico para o titular dos dados como também para os pesquisadores, posto que, colendo os dados com o consentimento do usuário, eles terão mais facilidade e certeza quanto a veracidade dos dados, evitando a propagação de dados caluniosos". [*Nicole Oliveira*]

Autor da proposta: *Daniel Astone* e *Nicole Oliveira.*

(D) A exceção da regra do consentimento especial para fins de pesquisa deve somente valer para órgãos públicos que tenham competências legais específicas, como o IBGE.

"*Caso contrário, a dissociação será obrigatória ou o consentimento deverá ser expresso*".

Autor da proposta: *Tagwato.*

(E) A lei deve tornar a dissociação dos dados obrigatória em casos de pesquisas.

"Caso contrário, seria uma brecha para empresas terem acesso a dados públicos ou de seus parceiros comerciais, com o subterfúgio de finalidade estatística ou de pesquisa".

Autor da proposta: *TV Aberta + Merchant = Peculato.*

(F) A lei deve restringir a exceção à regra do consentimento especial para dados sensíveis para as pesquisas estatísticas, mas abranger a pesquisas de mercado.

"Esta alínea deve excluir do seu rol as pesquisas estatísticas e incluir as pequisas de mercado. Dessa forma, torna-se mais clara a exceção feita na lei em benefício das pesquisas históricas, científicas e de mercado".

Autor da proposta: *ABEP.*

Sugestões de redação:

Autor da sugestão: *Associação da Liberdade Religiosa e Negócios.*

[MODIFICAÇÃO] c) Realização de pesquisa histórica, genealógica, artística, científica, cultural ou acadêmica, estatística ou de interesse público, garantidas as medidas de segurança aplicáveis;

Autor da sugestão: *Prof. Marcos.*

[MODIFICAÇÃO] c) realização de pesquisas históricas ou científicas que tenham sido aprovadas por conselho de ética de instituição reconhecida pelo MEC;

4.10.5. Exceção à regra de consentimento especial para dados sensíveis para exercício regular de direitos em processo judicial ou administrativo

Propostas avulsas para a regulação deste tema:

(A) A lei deve apenas criar uma exceção à regra de consentimento especial para exercício regular de direitos em processo judicial, não administrativo.

Autor da proposta: *Claro.*

4.10.6. Exceção à regra de consentimento especial para dados sensíveis para proteção da vida ou da incolumidade física do titular ou de terceiros

Propostas avulsas para a regulação deste tema:

(A) Uma exceção à regra de consentimento especial para dados sensíveis para proteção da vida ou da incolumidade física do titular ou de terceiros dá margem à realização de atividades de vigilância pelo Estado sobre os indivíduos.

Autor da proposta: *ABRANET.*

4.10.7. Exceção à regra de consentimento especial para dados sensíveis para tutela da saúde

Propostas avulsas para a regulação deste tema:

(A) Uma exceção à regra de consentimento especial para dados sensíveis para tutela da saúde dá margem à realização de atividades de vigilância pelo Estado sobre os indivíduos.

"Sugerimos exclusão ou reformulação. O inciso dá margem à realização de atividades de vigilância pelo Estado sobre os indivíduos".

Autor da proposta: *ABRANET.*

(B) Não deve existir uma exceção à regra de consentimento especial para dados sensíveis para tutela da saúde.

"Essa alínea deve ser suprimida. Não concordo com esse tipo de exposição sem o consentimento, mesmo que por profissionais da área específica. O indivíduo deve escolher como será o seu tratamento e à quem de confiança apresentar seus ditos dados sensíveis".

Autores da proposta: *Náthaly Morgani* e *Gabriela Martins.*

4.10.8. Novas propostas sobre exceções à regra de consentimento especial para dados sensíveis

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar uma exceção à regra de consentimento especial para garantir o uso de dados sensíveis na execução de procedimentos pré-contratuais e/ou contratuais em que o titular dos dados integre a relação jurídica.

"A inclusão da alínea se faz necessária para manter o equilíbrio com os termos do artigo 11. Este artigo estabelece a dispensa de consentimento para execução de procedimento pré-contratuais ou contratuais.

Esta dispensa se faz necessária também no caso de dados sensíveis, muitas vezes o responsável precisará dar tratamento a dados sensíveis para cumprir procedimentos pré-contratuais ou obrigações relacionadas a um contrato, não sendo exigível consentimento específico". [*Febraban*]

"Deve ser incluída entre as hipótese do inciso II uma que se refira à necessidade de tratamento para fins de conclusão ou execução de contrato. Não há nas hipóteses de tratamento de dados do inciso II uma que se refira à necessidade de tratamento para fins de conclusão ou execução de um contrato. Dados sensíveis, muitas hipótese, dentre elas nos seguros de pessoas ou de saúde, são de fundamental importância como a correta análise do risco e mesmo para o pagamento de eventuais indenizações.

Há hipótese em que a seguradora deve requisitar os dados concernentes ao estado de saúde do futuro segurado antes da execução do contrato e mesmo no decorrer do contrato quando há a necessidade de a fim de que possa efetuar o reembolso dos gastos realizados, o que, aliás, é a razão de existir dessa atividade". [*CNseg*]

Autor da proposta: *Fiesp, Febraban* e *CNseg.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[INCLUSÃO] nova alínea - execução de procedimentos pré-contratuais e/ou contratuais em que o titular dos dados integre a relação jurídica;

Autor da sugestão: *Febraban.*

[INCLUSÃO] nova alínea - execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 7º;

Autor da sugestão: *CNseg.*

[INCLUSÃO] nova alínea - execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular;

4.10.9. Quem pode tratar dados sensíveis? A quem a lei vai tutelar?

Propostas avulsas para a regulação deste tema:

(A) A definição de dados sensíveis deve ser restringida para que a aplicabilidade de seu regime especial não atinja operadores que não tenham consciência sobre a natureza dos dados.

"Este dispositivo é problemático já que nem sempre o operador tem consciência sobre a natureza das informações durante o tratamento de dados. Diante disso, sugerimos que a definição de dados sensíveis não seja tão ampla, com foco na revelação de dados sensíveis que podem resultar em prejuízos concretos aos titulares".

Autores da proposta: *ITI* e *Fiesp.*

4.10.10. Vedação ao tratamento de dados pessoais sensíveis "em detrimento do titular"

A discussão neste dispositivo girou em torno do termo "em detrimento do titular". Vários participantes, dentre eles *ITI*, *ABEMD* e *ABDTIC*, chamaram a atenção para a necessidade de melhor definir o termo. Segundo eles, o modelo de negócio de várias empresas de utilizar o tratamento de dados para criar de perfis de usuários ou analisar riscos acaba por lidar com informações que, em algumas situações, podem causar efeitos adversos aos titulares.

Diante dessa preocupação e das várias interpretações possíveis para o termo "em detrimento do titular", os participantes sugeriram ora a exclusão, ora a modificação do parágrafo:

Propostas avulsas para a regulação deste tema:

(A) Não deve existir uma vedação ao tratamento de dados pessoais sensíveis "em detrimento do titular".

"Acreditamos que não é bom para a indústria a vedação dessa possibilidade, por isso, defendemos a exclusão desse artigo ou a elaboração de uma legislação específica que permite o tratamento de dados para esse fim".

Autores da proposta: *ABRANET, Brasscom* e *Câmara BR.*

(B) A vedação ao tratamento de dados pessoais sensíveis "em detrimento do titular" deve conter uma exceção para liberar modelos de negócios baseados em estudos atuariais.

"*O parágrafo deve ser alterado para garantir a proteção do modelo de negócio de grande parte das empresas de internet que se baseia no uso de dados dos usuários*". [*Fiesp*]

"Tal como posto, o parágrafo pode ter impactos negativos no setor de seguros na medida em que a lógica do seguro se funda na generalização e na discriminção, 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.

Dados sensíveis podem ser usados para aumentar (ou reduzir) o valor do prêmio a ser pago e este tratamento de dados, inerente ao negócio dos seguros, poderia ser considerado "em prejuízo do titular". [*CNseg*]

Autores da proposta[22]: *Fiesp* e *CNseg.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica e quanto à liberdade dos modelos de negócio baseados em estudos atuariais.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] § 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.

[22] Como pode se observar nas sugestões de redação abaixo, *CNseg* e *Fiesp* encaminharam sua proposta de maneiras diversas.

4.10.11. Quem pode dirimir dúvidas acerca da sensibilidade de dados pessoais?

Propostas avulsas para a regulação deste tema:

(A) O órgão competente deve abarcar essa função.

"Sugerimos a inclusão deste parágrafo 4º, já que este é necessário para criar uma porta aberta para que os usuários tenham esclarecidas dúvidas quanto aos pontos da lei, evitando equívocos desnecessários".

Autores da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[INCLUSÃO] §4º O órgão regulador fiscalizador deverá ser consultado pelos interessados a fim de dirimir dúvidas acerca da sensibilidade dos dados pessoais;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~12~~ 11. É vedado o tratamento de dados pessoais sensíveis, salvo:

I – com fornecimento de consentimento ~~especial~~ inequívoco, expresso e específico pelo titular:

a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e

b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento ~~desta espécie de dados; ou~~**.**

II – sem fornecimento de consentimento do titular, ~~quando os dados forem de acesso público irrestrito, ou~~ nas hipóteses em que for indispensável para:

a) cumprimento de uma obrigação legal pelo responsável;

b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a ~~dissociação~~ anonimização dos dados ~~pessoais;~~ pessoais sensíveis;

d) exercício regular de direitos em processo judicial ou administrativo;

e) proteção da vida ou da incolumidade física do titular ou de terceiro; ou

f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias. § 1º O disposto neste artigo aplica-se a qualquer tratamento de dados pessoais capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º O disposto no item 'c' do inciso II somente se aplicará caso as atividades descritas não estejam vinculadas a atividade comercial, de administração pública, investigação criminal ou inteligência, garantindo-se, sempre que possível, a anonimização dos dados pessoais.

§ 4º Nos casos de aplicação do disposto nos itens 'a' e 'b' do inciso II pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do ~~§1o do~~ art. ~~6o~~ 24.

4.11. Medidas adicionais de segurança ou de proteção a dados pessoais sensíveis

REDAÇÃO LEVADA A DEBATE

Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.

§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.

§ 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.

O artigo 13 traz à tona a discussão acerca de possíveis medidas adicionais de segurança a serem determinadas pelo órgão competente. Neste ponto, durante o debate na plataforma, ficou clara a preocupação das empresas com a possibilidade de o órgão competente, ao visar à melhor proteção do usuário, estabelecer medidas excessivamente onerosas ou desproporcionais para as empresas.

Em razão disso, podemos observar que as contribuições da maioria dos participantes buscam balizar a faculdade do órgão competente de impor medidas de segurança ou, até mesmo, sugerir que tais medidas sejam implementadas somente através de lei.

4.11.1. O órgão competente deverá ter competência para estabelecer medidas adicionais de segurança e de proteção de dados sensíveis?

Respostas controversas coletadas na plataforma de debate:
(A) Não. Não seria razoável que qualquer órgão estabeleça medidas adicionais de segurança e de proteção aos dados pessoais sensíveis estabelecidos pela Lei sem submeter, obrigatoriamente, as novas medidas a processo de consulta pública. Tal atribuição deve ser do legislativo. **Quem defendeu isso?** *Brasscom, SindiTeleBrasil e ABRANET*.
(B) Sim, mas tais medidas devem sem flexíveis. Medidas impostas através deste artigo devem ser suficientemente flexíveis, de forma que as organizações se adequem às medidas apropriadas segundo a sua estrutura e à natureza dos dados sensíveis. **Quem defendeu isso?** *ITI e Câmara BR.*
(C) Sim, mas tais medidas devem respeitar o disposto no artigo 42. O artigo deve fazer menção ao artigo 42 que garantirá que a imposição de novas normas de proteção e medidas de segurança respeitará critérios de razoabilidade, proporcionalidade e necessidade traduzidos no artigo. **Quem defendeu isso?** *ABEP*.
(D) Sim, mas tais medidas devem respeitar o contexto de utilização dos dados e visar o

interesse público.

Essa previsão é condizente com os desafios do mundo digital e está em acordo com várias jurisdições, particularmente europeias, nas quais a proteção ao titular é mais elevada.

Para estabelecer as medidas adicionais de segurança, a autoridade deverá: considerar diferentes contextos em que dados sensíveis são utilizados e balizar essa utilização para que ocorra apenas em situações de interesse público e sem prejudicar o sujeito a que tais dados se referem, garantindo, portanto, que práticas adequadas de anonimização e segurança sejam implementadas.

Quem defendeu isso? *Joana Varon.*

Propostas avulsas para a regulação deste tema:

(A) A lei deve adotar a necessidade de ordem judicial ou consentimento do titular para que dados sensíveis sejam entregues ao governo como medida de proteção.

"Dados pessoais sensíveis só deverão ser entregues ao governo mediante consentimento ou ordem judicial que assim determine. O órgão de governo deve apenas requisitar melhores medidas de proteção, sem contudo exigir a guarda e/ou administração de tais dados".

Autores da proposta: *ABDTIC.*

4.11.2. Necessidade de autorização prévia do órgão competente para determinadas modalidades de tratamento de dados sensíveis a serem definidas no regulamento

Propostas avulsas para a regulação deste tema:

(A) A lei não deve prever a necessidade de autorização prévia do órgão competente para modalidades de tratamento de dados pessoais sensíveis.

"Sugerimos a exclusão do parágrafo. Entendemos que não caberia ao órgão competente proibir ex ante o tratamento de dados, mas sim de fiscalização posterior, coibindo abusos que eventualmente tenham sido realizados".

Autores da proposta: *Brasscom, ITI* e *Fiesp.*

(C) A lei deve dispor que as modalidades de tratamento de dados pessoais sensíveis definidas pelo órgão competente também dependerão da obtenção de consentimento especial do titular.

Autor da proposta: *Proteste.*

Sugestões de redação:

Autor da sugestão: *Proteste.*

[MODIFICAÇÃO] § 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, bem como de consentimento especial do titular, nos termos do regulamento.

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] § 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento, levando-se em consideração, dentre outros princípios, o quanto disposto no artigo 6º, inciso III.

4.11.2. Tratamento de dados biométricos e órgão competente

Por um lado, alguns participantes ressaltaram a forte ligação da proteção dos dados biométricos com a proteção dos direitos dos titulares e, por outro, os usos importantes dos dados biométricos para proteção do consumidor.

Propostas avulsas para a regulação deste tema:

(A) A lei precisa trazer uma definição de "dados biométricos".

"Dados biométricos devem ser definidos em lei. Além disso, deve-se tomar cuidado para não limitar o uso importantes de dados biométricos, tais como o uso para autenticação do consumidor".

Autores da proposta: *ITI, RafaelIC e Fiesp.*

(B) A lei deve definir que bens, produtos ou serviços não podem estar condicionados à coleta de dados biométricos.

"*Uso de dados biométricos deve ser feito pelas pessoas exclusivamente de acordo com a vontade dos titulares dos dados. Entes públicos e privados não deverão poder condicionar o acesso a bens, produtos e serviços a coleta de dados biométricos*".

Autor da proposta: *Rodrigo Veleda.*

(C) A lei deve considerar dados biométricos sempre ser como dados pessoais sensíveis.

Os defensores desta proposta argumentam que trata-se de matéria diretamente relacionada à segurança e integridade física do titular.

Autores da proposta: *Bruno Diego, TV Aberta + Merchant = Peculato* e *Joana Varon.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~13~~ 12. ~~Órgão~~ O órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento**,** ou solicitar a apresentação de relatório de impacto à privacidade.

Art. 13. Os dados anonimizados serão considerados dados pessoais para os fins desta Lei quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido.

§ 1º ~~A realização~~ Poderão ser igualmente considerados como dados pessoais para os fins desta Lei os dados utilizados para a formação do perfil comportamental de ~~determinadas modalidades~~ uma determinada pessoa natural, ainda que não identificada.

§ 2º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança.

§ 3º O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento.

Art. 14. O tratamento de dados pessoais ~~sensíveis poderá ser condicionada à autorização prévia~~ de ~~órgão competente~~ criança e pessoa absolutamente incapaz, nos termos ~~do regulamento~~ da lei, somente pode ser realizado mediante consentimento dos responsáveis legais e no seu melhor interesse.

Parágrafo único. ~~**§ 2º**~~ O tratamento de dados pessoais ~~biométricos será disciplinado por órgão competente~~ de adolescente e pessoa relativamente incapaz observará as seguintes condições:

I – autorização condicionada à supervisão, ~~que disporá sobre hipóteses em que dados biométricos serão considerados~~ assistência ou anuência do responsável legal; e

II – respeito à sua condição pessoal, podendo os responsáveis legais revogar o consentimento para tratamento de dados pessoais ~~sensíveis~~ a qualquer tempo.

4.12. Término do tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade específica almejada;

II - fim do período de tratamento;

III – comunicação do titular; ou

IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.

Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.

4.12.1. Término do tratamento de dados pessoais por finalidade alcançada

Propostas avulsas para a regulação deste tema:
(A) A lei deve dispor que o término do tratamento de dados pessoais deve ocorrer com o alcance da finalidade "legítima". Segundo os participantes que defenderam essa proposta, a finalidade precisa ser inserida dentro de um contexto moderno. Muitas vezes uma finalidade "legítima" surgiria durante o processamento de dados. **Autores da proposta**: *ABRANET* e *GSMA.*
(B) A lei deve dispor que o término do tratamento de dados pessoais deva se reduzir a três hipóteses: desejo soberano do titular; término da duração estipulada; ou comprovada

violação à lei.

Defende que o inciso relativo ao término por finalidade alcançada seja suprimido. "*Não se deve, portanto, abrir a possibilidade para que agente estatal decida subjetivamente sobre o término do tratamento*".

Autor da proposta: *SindiTeleBrasil.*

Sugestões de redação:

Autor da sugestão: *ABRANET.*

[MODIFICAÇÃO] I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade legítima;

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] I – quando os dados não forem mais necessários ou pertinentes para propósitos originais ou finalidades compatíveis;

4.12.2. Período de tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) Deve ser aberta a hipótese legal de tratamento de dados por prazo indeterminado e/ou restrito ao poder do órgão competente em estabelecer prazos máximos para tratamento de dados.

Para os defensores desta proposta a existência de períodos máximos para o tratamento de dados deveria ser uma dentre outras possibilidades, tal como a hipótese de tratamento por prazo indeterminado, e não uma obrigação. A inexistência de tal possibilidade seria uma intromissão estatal excessiva em relação à liberdade econômica.

Afirmam que é "*um caso em que há excesso de poder conferido à autoridade competente*".

"Não é apropriado estabelecer períodos máximos de tratamento. Há, ao contrário, uma necessidade de flexibilização no que diz respeito ao tratamento de dados. Os consumidores e empresas utilizam diversos serviços com a expectativa de que seus dados sejam gravados e processados por um prazo indeterminado; esse dispositivo vai de encontro a essas expectativas". [*ITI*]

"O ideal seria que os dados fossem processados por prazo indeterminado para fins negociais, sem limitar a segurança ou proteção. Ademais, recomenda-se que, após o fim do prazo máximo, os dados sejam eliminados" [*Fiesp*]

Autores da proposta: *Fiesp, ITI, MPA, Brasscom, Câmara BR, ABRANET, ABDTIC, CNseg, GSMA, US*

Business Council e *SindiTeleBrasil.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto no artigo 10, §4º desta lei ou disposição em legislação específica.

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] Parágrafo único. Órgão competente pode, em determinados casos, estabelecer períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica, ou conforme acordado em acordos contratuais.

Autor da sugestão: *ABDTIC.*

[MODIFICAÇÃO] Parágrafo Único. Órgão competente poderá estabelecer períodos máximos para o tratamento de dados pessoais, nos casos previstos em lei.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] 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.

4.12.3. Término do tratamento de dados pessoais por comunicação do titular

Propostas avulsas para a regulação deste tema:

(A) O término do tratamento de dados pessoais por comunicação do titular só deve ocorrer quando este não for incompatível com os interesses legítimos do responsável.

"Tendo em vista a necessidade de flexibilização da concepção de "finalidade" do tratamento de dados, as regras sobre fim do tratamento devem permitir o desenvolvimento de novos produtos e serviços, desde que não haja prejuízo à privacidade dos consumidores. Sendo assim, propomos nova redação".

Autores da proposta: *GSMA.*

(B) O término do tratamento de dados pessoais por comunicação do titular só deve ocorrer

quando sobrevierem razões preponderantes e legítimas.

"Proposta de nova redação se faz necessária para evitar o abuso de direito por parte dos titulares, a exemplo, inclusive, do que foi estabelecido na diretiva europeia 95/46/EC, art. 14".

Autores da proposta: *Brasscom.*

(C) A lei deve prever um prazo para que o término do tratamento ocorra após a comunicação do titular.

"Na hipótese de o titular dos dados revogar consentimento, em quanto tempo a empresa deverá deletar os dados? Talvez seria interessante ter uma provisão estabelecendo um prazo para deletar, sendo o usuário notificado disso".

Autores da proposta: *Danielekfontes.*

Sugestões de redação:

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] III – a pedido do titular, quando tal pedido não for incompatível com os interesses legítimos do responsável e quando a continuidade do processamento não puser em risco o titular;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] III – comunicação do titular, quando houver razões preponderantes e legítimas para a solicitação do término do tratamento;

4.12.4. Término do tratamento de dados pessoais por determinação do órgão competente

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever que a determinação de término do tratamento de dados pessoais precisa respeitar razoabilidade e proporcionalidade.

Autor da proposta: *ABRANET.*

(B) A lei deve prever que a determinação de término do tratamento de dados pessoais somente poderá ocorrer caso não haja outro remédio mais adequado para sanção.

Autor da proposta: *Brasscom.*

Sugestões de redação:
Autor da sugestão: *ABRANET.* **[MODIFICAÇÃO]** IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar, ressalvados os princípios da razoabilidade e da proporcionalidade;
Autor da sugestão: *Brasscom.* **[MODIFICAÇÃO]** IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar, desde que não haja outro remédio mais adequado para a sanção;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~14~~ 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no art. 9, § 5º; ou

IV – determinação ~~de~~ do órgão competente**,** quando houver violação ~~de dispositivo legal ou regulamentar~~ da legislação em vigor a respeito.

Parágrafo único. ~~Órgão~~ O órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.

4.13. Cancelamento e conservação de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal pelo responsável;

II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou

III – cessão a terceiros, nos termos desta Lei.

Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.

Neste artigo e em seus incisos, foram sugeridas novas hipóteses de autorização para conservação dos dados, assim como foram feitas observações acerca do significado de término do tratamento e de cancelamento.

4.13.1. Dever de cancelamento: cumprimento de dever legal, legítimo interesse, dissociação e cancelamento definitivo

Propostas avulsas para a regulação deste tema:

(A) O cancelamento de dados pessoais apenas deve ocorrer quando houver expressa manifestação do titular ou quando o término do tratamento decorrer de violação de dispositivo legal ou regulamentar.

"Isso porque é muitas vezes é necessário manter os dados armazenados, como forma de evitar os casos de fraudes nas empresas quando os clientes retomam a relação contratual".

Autores da proposta: *SindiTeleBrasil.*

(B) A lei deve permitir a conservação dos dados pessoais em caso de legítimo interesse do responsável e de acordo de boa-fé.

"A conservação de dados para fins exclusivamente cadastrais pode ajudar a prevenir fraudes." [*ABEMD*]

"Sugerimos a exclusão do artigo 15. Após o término da relação contratual, é muitas vezes necessário conservar os dados pessoais, para resguardar direitos daquele que faz o tratamento dos dados, nas hipóteses de ações judiciais onde muitas vezes o ônus da prova é dele, bem como a fim de se verificar informações e evitar, p. ex., casos de fraudes de terceiros". [*Claro*]

Autores da proposta: *ABEMD, GSMA* e *Claro.*

(C) A lei deve permitir a conservação dos dados pessoais que tiverem sido razoavelmente anonimizados.

Autores da proposta: *ITI.*

(D) A lei não deve dispor sobre cancelamento de dados pessoais, e sim, sobre sua dissociação.

"*Sugere-se a substituição do termo cancelados pelo termo dissociação a fim de dar coerência com a definição dada no inciso XIV do artigo 5º".*

Autores da proposta: *Fiesp.*

(F) A lei deve obrigar o cancelamento a ser definitivo, sem possibilidade de novo acesso aos dados.

Autores da proposta: *Giovanna Carloni.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 15. Os dados pessoais serão dissociados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 15. Após o término do tratamento dos dados pessoais, o responsável deve proceder a sua eliminação quando o titular manifestar formalmente tal desejo ou quando o término decorrer de comprovada violação de dispositivo legal ou regulamentar.

4.13.2. Conservação de dados pessoais para fins de pesquisa

Propostas avulsas para a regulação deste tema:

(A) A lei deve permitir a conservação de dados pessoais para fins de pesquisas de mercado e obrigar o cancelamento no caso de pesquisas estatísticas.

"Dessa forma, torna-se mais clara a exceção feita na lei em benefício das pesquisas históricas, científicas e de mercado".

Autores da proposta: *ABEP.*

(B) A lei deve permitir a conservação de dados suficientes para que seja possível manter um acervo de informações sobre a relação contratual entre o responsável e o titular.

"Sugere-se que seja permitida a manutenção das informações suficientes para que seja possível manter um acervo de informações a respeito das relações que as entidades mantiveram com seus clientes, incluindo, exemplificadamente, as informações contratuais básicas, os tipos de produtos e volumes contratados, dados de contato para eventual retomada comercial, entre outras informações, respeitados, sempre, os princípios gerais da Lei".

Autores da proposta: *Vivo.*

(C) A conservação de dados pessoais também deve ser ampliada para fins de pesquisas "genealógicas, artísticas, culturais, acadêmicas e de interesse público".

"Anteprojeto deve manter a autorização da conservação dos dados pessoais com finalidade de pesquisa histórica, científica ou estatística. Contudo, entendemos que este conceito deve ser ampliado também para fins de pesquisas genealógicas, artísticas, culturais ou acadêmicas, e de interesse público".

Autores da proposta: *Associação da Liberdade Religiosa e Negócios.*

(D) A lei deve obrigar que dados pessoais usados em pesquisas sejam "anonimizados", não "dissociados".

Segundo defensores desta proposta, seria mais adequado que a lei se refira ao processo mais genérico para abarcar também outras técnicas que existem ou venham a existir.

Autores da proposta: *Veridiana/Intervozes* e *Proteste.*

(E) A lei deve vedar a utilização de dados sensíveis em pesquisas estatísticas "de interesse privado".

"As utilização de dados sensíveis em pesquisas estatísticas não poderão ser utilizadas para o interesse privado. Nossa proposta se baseia na garantia de que empresas não se utilizarão dos dados para estatísticas de interesse privado".

Autores da proposta: *Proteste.*

(F) A lei deve tornar a dissociação uma condição para o uso de dados pessoais conservados em pesquisas.

"A dissociação dos dados deve ocorrer sempre. Substituir o: sempre que possível, a dissociação dos dados pessoais. Para: "Sempre com a dissociação dos dados pessoais". Por ser pesquisa ou estatística, imagino que estarão envolvidos os dados de milhares ou milhões de indivíduos. Seria uma brecha para empresas terem acesso a dados públicos ou de seus parceiros comerciais, com o subterfúgio de finalidade estatística ou de pesquisa".

Autores da proposta: *TV Aberta + Merchant = Peculato.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] II – manutenção do acervo de registros, pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou;

Autor da sugestão: *Associação da Liberdade Religiosa e Negócios.*

[MODIFICAÇÃO] II – pesquisa ou conservação de arquivos ou registros históricos, genealógicos, artísticos, científicos, culturais ou acadêmicos, estatísticos ou de interesse público, garantidas as medidas de segurança aplicáveis;

Autor da sugestão: *Proteste.*

[MODIFICAÇÃO] II – pesquisa histórica, científica ou estatística vinculada à política pública, garantida, sempre que possível, a anonimização dos dados pessoais;

4.13.3. Conservação de dados para cessão a terceiros

Na discussão sobre este inciso, a principal dificuldade apresentada foi a definição do termo "cessão a terceiros" (*SindiTeleBrasil* e *ITI*), a *Fiesp* sugeriu a delegação da definição do termo ao órgão competente. Os participantes também se manifestaram no sentido de buscar formas de proteção do usuário em caso de cessão ou mesmo de desvincular a cessão a terceiros da autorização para conservação de dados.

Propostas avulsas para a regulação deste tema:

(A) A lei deve vedar a cessão de dados pessoais a terceiros sem autorização do titular.

"A cessão deveria depender de autorização do usuário para se concretizar. Essa cessão deveria obrigatoriamente ter que receber nova autorização dos usuários, principalmente se a finalidade, adequação e outros princípios se tornarem diferentes pelo cessionário.

A exceção prevista nesse inciso viola o princípio da boa-fé, o qual estabelece deveres de conduta, dentre eles, o dever de informação , sendo necessário que o responsável pelo tratamento dos dados pessoais informe ao usuário quem acessa e utiliza suas informações.

Portanto, deveria ser exigida a autorização do usuário para que os dados pessoais informados a determinada empresa sejam repassados por ela a outas empresas, pois da maneira como está previsto, permitindo o repasse de dados a empresas/terceiros desconhecidos, está-se violando o

direito de informação e aumentando a vulnerabilidade dos usuários".

Autores da proposta: *Flávio Costa* e *Marina.*

(B) A lei não deve permitir a conservação de dados pessoais com a finalidade de cessão a terceiros.

"A cessão de dados a terceiros não deveria ser uma causa para a conservação de dados pessoais após o término do tratamento. Se porventura tais dados foram transferidos a terceiros, respeitada a disciplina de consentimento aplicável a essas operações, esses terceiros também estarão sujeitos a regra de cancelar os dados recebidos quando findado o tratamento. Por outro lado, o caso de cessão a terceiros por força de obrigação legal, como as previstas no Marco Civil da Internet quanto à guarda e disponibilização de registros, já está contemplado no art. 15, I".

Autora da proposta: *Veridiana/Intervozes.*

4.13.4. Novas hipóteses de conservação de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve permitir a conservação de dados pessoais para comprovação de cumprimento de obrigações contratuais e extracontratuais perante terceiro e/ou perante o próprio titular.

Autor da proposta: *Vivo.*

(B) A lei deve permitir a conservação de dados pessoais se forem dados anonimizados ou quando isso for expressamente requerido ou consentido pelo titular.

"Os novos incisos propostos se baseiam na ideia de que novos usos de dados pessoais em vários campos do conhecimento ainda estão sendo descobertos e, portanto, caso as hipóteses do art. 15 sejam demasiadamente restritivas, o Brasil corre o risco de inibir ou inviabilizar o processo de inovação e o desenvolvimento benéfico decorrente do uso de (IV) dados anonimizados ou baseado na escolha ou (V) consentimento informado do titular".

Autor da proposta: *Brasscom.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[INCLUSÃO] IV – conservação das evidências necessárias e suficientes para comprovar o cumprimento de obrigações perante terceiros e o titular;

Autor da sugestão: *Brasscom.*

[INCLUSÃO] IV – quando forem processados de tal forma que não se tratem mais de dados pessoais;

V – quando o titular assim consentir ou expressamente requerer;

4.13.5. A possibilidade de o órgão competente estabelecer hipóteses específicas de conservação de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei não deve abrir a possibilidade de o órgão competente estabelecer hipóteses de conservação de dados pessoais.

"O parágrafo deveria ser excluído. Se houver interesse do Estado na conservação de dados pessoais, deverá obter autorização para tal conservação por meios legais e, então, mantê-los por sua conta" [*ABRANET*].

Autores da proposta: *ABRANET, ABDTIC e Câmara BR.*

(B) A lei deve garantir que a possibilidade de o órgão competente em estabelecer novas hipóteses de conservação de dados pessoais leve em conta a natureza dos dados e da organização que realiza o tratamento.

Autores da proposta: *ITI.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[INCLUSÃO] § 2º Caso não seja possível a dissociação, os dados pessoais serão cancelados após o término do seu tratamento, ressalvadas as disposições de conservação deste artigo.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~15~~ 16. Os dados pessoais serão ~~cancelados~~ eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal ~~pelo~~ do responsável;

II – pesquisa histórica, científica ou estatística, garantida, ~~sempre que~~ quando possível, a ~~dissociação~~ anonimização dos dados pessoais; ou

III – ~~cessão~~ transferência a terceiros, ~~nos termos desta~~ desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.

Parágrafo único. ~~Órgão~~ O órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.

4.14. A titularidade dos dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Propostas avulsas para a regulação deste tema:
(A). Para garantir os direitos fundamentais enunciados, a lei deve tornar regra geral o uso de ordem judicial para acesso a dados pessoais. **Autor da proposta**: *Rodrigo Veleda.*
(B). A lei deve dispor que o titular dos dados pessoais não poderá arguir da própria torpeza. *"Deve ser expresso no artigo a impossibilidade de arguição da própria torpeza. Ou seja, o titular dos dados, ao utilizar a rede deverá também se limitar aos mesmos direitos alheios, na mesma medida que lhes é dado".* **Autora da proposta**: *Kaliny Aglay.*
(C). A lei deve enunciar mais especificamente quais os direitos do titular dos dados pessoais que são decorrentes de suas garantias fundamentais.

"Este ponto deve tratar de direitos decorrentes de forma direta do assunto tratado, por exemplo, o direito à confirmação da existência de dados. Sugere-se também que os princípios tratados neste artigo (liberdade, intimidade e privacidade) sejam elencados no início da lei e que, nesta seção, seja feita referência ao supra estabelecido".

Autor da proposta: *ABRANET.*

(D). A lei deve também reconhecer o direito fundamental à inviolabilidade à honra e à imagem.

Autor da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais previstos na Constituição Federal.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~16~~ 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

4.15. Direitos do titular dos dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 17. O titular dos dados pessoais tem direito a obter:

I – confirmação da existência de tratamento de seus dados;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados; e

IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

§1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, alegando descumprimento ao disposto nesta Lei.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2o, o responsável enviará ao titular, em até sete dias a partir da data do recebimento da comunicação, resposta em que poderá:

I – comunicar que não é agente de tratamento dos dados; ou

II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 4º A providência de que trata o § 2o será realizada sem ônus para o titular.

§ 5º 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.

4.15.1. Considerações gerais sobre a garantia de direitos ao titular dos dados pessoais

Propostas avulsas para a regulação deste tema:
(A) A garantia de direitos ao titular de dados pessoais deve estar balizada pela "razoabilidade e disponibilidade de recursos". *"Propomos nova redação em razão da necessidade de balancear o exercício dos direitos dos titulares com parâmetros de razoabilidade e disponibilidade de recursos, a exemplo do que já ocorre na europa: art. 12º da Diretiva Europeia 95/46 CE".* **Autor da proposta**: *Brasscom.*
(B) A garantia de direitos ao titular de dados pessoais não deve se resumir a um rol taxativo, mas incluir direitos previstos em todo o texto legal. **Autores da proposta**: *Fiesp e SindiTeleBrasil.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 17. O titular dos dados pessoais tem direito a obter, com base na razoabilidade e disponibilidade de recursos:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 17. O titular dos dados pessoais tem direito a obter, além das informações previstas no artigo 10 desta lei:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 17. Sem prejuízo dos demais direitos estabelecidos nesta Lei, o titular dos dados pessoais tem direito a obter:

4.15.2. Direito de confirmação da existência de tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) O direito de confirmação da existência de tratamento de dados pessoais deve ser ampliado para abarcar o direito do titular ser notificado quando do tratamento de seus dados pessoais.

Para as autoras da proposta, o direito deve abranger também o direito de ser informado, "*mesmo nos casos de exceção ao consentimento, desde que tal informação não afete a finalidade da coleta, sobre o tratamento de seus dados, bem como sobre a política de privacidade para utilização dos mesmos*".

Autoras da proposta: *Joana Varon* e *Gabriela Martins.*

4.15.3. Direito de acesso aos dados

Propostas avulsas para a regulação deste tema:

(A) A lei deve limitar o direito do titular de acesso a seus dados, caso isso não possa ocorrer sem a divulgação concomitante de dados de terceiros.

"Existem circunstâncias em que não é possível fornecer a um titular informações sobre seus próprios dados sem a divulgação de informações que pertençam a outros titulares (por exemplo, quando as

informações fazem parte de arquivos ou bases de dados que não podem ser modificados para segregar informações de um indivíduo).

Isso deve ser levado em conta ao se estabelecer o direito de acesso de dados de uma determinado titular e, portanto, recomendamos que o artigo 17, II seja alterado de forma a incluir tal exceção". [*US Business Council*]

Autores da proposta: *BSA e US Business Council.*

(B) A lei deve determinar o formato do exercício do direito de acesso a dados pessoais.

"*O acesso aos dados pessoais deve-se dar mediante a obtenção de uma cópia em formato estruturado e em padrão aberto, sob pena de, caso contrário, tal direito não ser exequível por conta de um formato ilegível ou um padrão não executável em certos sistemas operacionais*".

Autor da proposta: *GPoPAI.*

(C) A lei deve restringir o direito de acesso ao "acesso razoável" a dados pessoais.

"O conceito da 'razoabilidade' deve ser incluído nesta disposição para que o usuário tenha o direito de obter o "acesso razoável". Desta forma, busca-se relativizar esse direito de acesso de forma que ele não exija coleta de mais dados para a autentificação do usuário do que aqueles necessários para a prestação de serviços. Da mesma forma, se a autenticação do usuário exigir mais dados pessoais do que aqueles que a organização possui, a organização deve ter a capacidade de recusar o pedido de acesso".

Autor da proposta: *ITI.*

Sugestões de redação:

Autor da sugestão: *BSA.*

[MODIFICAÇÃO] II – acesso aos dados, a menos que tal acesso não seja viável sem a revelação de informações pertencentes a outros titulares de dados;

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] II – acesso razoável a dados, exceto quando tal acesso coloca em risco a privacidade e a segurança de dados pessoas relativos a outra pessoa ou durante o curso de uma pesquisa clínica onde tal acesso poderia prejudicar a integridade da pesquisa;

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] II – acesso aos dados, mediante a obtenção de cópia eletrônica, em formato estruturado e padrão aberto, de todos os seus dados pessoais junto ao operador responsável pelo tratamento de dados pessoais;

4.15.4. Direito de correção de dados incompletos, inexatos ou desatualizados

Propostas avulsas para a regulação deste tema:

(A) A lei deve limitar o direito de correção de dados pessoais para permitir a conservação de dados para prevenção de fraudes, manutenção de registros dos serviços prestados e evitar infração a direitos de terceiros.

Autores da proposta: *ITI* e *Brasscom.*

(B) A lei deve deixar claro que o direito de correção se restringe a dados pessoais incorretos e não deverá prejudicar a liberdade de expressão[23].

Autor da proposta: *Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] III – correção de dados pessoais e informações gerais incompletas, inexatas ou desatualizadas; e;

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] III – correção de dados seus, se incompletos, inexatos ou desatualizados, desde que tal correção não prejudique direitos de terceiros ou obrigações legais ou contratuais do responsável; e;

4.15.5. Direito de dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados de forma ilícita

Propostas avulsas para a regulação deste tema:

(A) O direito de dissociação, bloqueio ou cancelamento de dados pessoais deve ser limitado à hipótese de dados pessoais tratados em desconformidade com a lei.

"Propomos a retirada dos termos desnecessários e excessivos. As palavras 'desnecessários' e 'excessivos' são amplas e podem conceder uma grande responsabilidade para as indústrias, pois elas serão responsáveis por definir quais informações são desnecessárias e quais são excessivas".

[23] Neste ponto nota-se uma preocupação com a possibilidade de o direito de correção de dados pessoais se tornar uma modalidade de "direito ao esquecimento".

[*Brasscom*]

Autores da proposta: *Câmara BR* e *Brasscom.*

(B) A lei deve facultar ao responsável pelo tratamento de dados pessoais o cancelamento de serviços prestados ao titular, caso o exercício do direito de dissociação, cancelamento ou bloqueio os afetem operacional ou economicamente.

"Este inciso deve esclarecer que o cancelamento de dados pode levar a interrupção total ou parcial do serviço ao usuário. Em consonância com o comentário do inciso III, podm haver situações em que há razões comerciais legítimas para manutenção dos dados, tais como: prevenção de fraudes e manutenção de registros". [*ITI*].

Autores da proposta: *Brasscom* e *ITI.*

(C) O termo "dissociação" deve ser substituído pelo termo "anonimização".

Autor da proposta: *Proteste.*

(D) A lei não deve garantir um direito de dissociação, bloqueio ou cancelamento de dados pessoais.

"Sugerimos a eliminação deste inciso. Dado que prevê-se neste dispositivo que o titular dos dados pode opor-se a todo o tempo ao tratamento dos seus dados pessoais, ou solicitar a dissociação/cancelamento de dados desnecessários, sendo que este tratamento já estaria dispensado de consentimento, podendo os dados da solicitação para cancelamento/dissociação serem essenciais à concretização do negócio/projeto em questão.

Ademais, é necessário às empresas manter um histórico de seus clientes de forma a evitar futuras fraudes caso o cliente retome a relação de consumo".

Autores da proposta: *Vivo.*

(E) A lei deve ampliar este direito para incluir a "remoção total" dos dados pessoais.

"*Incluir a remoção total dos dados, não apenas seu bloqueio, cancelamento ou dissociação. Cancelamento não parece ser a melhor designação para aquele que precisará se desfazer dos dados desnecessários*".

Autores da proposta: *Drica* e *Marcelo Crespo.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] IV – dissociação, bloqueio ou cancelamento de dados tratados em desconformidade com o disposto nesta Lei, ressalvados os princípios constitucionais da liberdade

de expressão e de imprensa, bem como o acesso à informação;

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] IV – dissociação, bloqueio ou cancelamento de dados tratados em desconformidade com o disposto nesta Lei;

Autor da sugestão: *Proteste.*

[MODIFICAÇÃO] IV – anonimização, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei;

4.15.6. Propostas de novos direitos do titular dos dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer o direito à portabilidade de dados pessoais.

"Sugerimos a criação de um novo inciso ao art. 17, elencando como um dos direitos a portabilidade pela qual o titular possa 'trocar' de prestador de serviço ou fornecedor de produto, levando com ele seus dados pessoais". [*GPoPAI*]

Autores da proposta: *GPoPAI* e *Proteste.*

(B) A lei deve garantir o direito à exclusão do banco de dados.

Autor da proposta: *Proteste.*

(C) A lei deve estabelecer o direito à informação do cidadão acerca do funcionamento da rede, da coleta de dados pessoais, das suas finalidades e usos.

"Deve-se, neste ponto, ter em mente a necessidade de educação do usuário e fazer menção ao direito de todo cidadão a saber o funcionamento da rede, como e quais dados são coletados e como e para que finalidade eles podem ser utilizados, de forma clara e simples".

Autor da proposta: *Fabricio Pessôa.*

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] V – obter a portabilidade através de transmissão, mediante sua requisição, dos seus dados pessoais para outro fornecedor de serviço ou produto, cuja técnica, modalidade e

procedimento poderão ser definidos pelo órgão competente ou por melhores práticas de mercado e, sem prejuízo, de revogar o seu consentimento nos termos do § 6º, do artigo 7.

Autor da sugestão: *Proteste.*

[INCLUSÃO] V – exclusão do banco de dados por interesse do titular;

VI – portabilidade por interesse do titular ou, sendo por interesse do responsável, ao consentimento prévio.

4.15.6. Oposição a tratamento realizado por hipótese de dispensa de consentimento

Propostas avulsas para a regulação deste tema:

(A) A lei não deve garantir um direito específico de oposição a tratamento realizado com fundamento em hipótese de dispensa do consentimento.

Os defensores desta proposta acreditam que a presença de outros direitos no texto legal tornam a medida excessiva. Argumentam que a oposição poderia prejudicar a concretização da prestação de serviços e que seria necessário a manutenção de um histórico de clientes a fim de evitar futuras fraudes.

Autores da proposta: *ABRANET, Câmara BR, Claro, Vivo e ABDTIC.*

(B) O titular que decidir se opor a tratamento realizado por hipótese de dispensa de consentimento deve comprovar a violação por parte do responsável.

"A substituição de 'alegando' por 'comprovando' é necessária porque o usuário, que tem o direito de se opor ao tratamento de seus dados, deve ser capaz de provar que o tratamento de seus dados não se enquadra nas hipóteses do artigo 11. Caso não seja obrigado a provar, este dispositivo acabará por servir de escudo para quem não quer que o responsável exerça seu direito de tratar os dados, sem o consentimento, quando possibilitado legalmente.

O cenário acima mostra-se mais claro quando se observa a situação na qual o responsável, no exercício de seu regular direito de cobrança, utiliza os dados do titular para propor ação judicial (art. 11, VI). Se o titular não provar que não se trata dessa situação, o responsável não pode ser inviabilizado de utilizar-se da dispensa legal do consentimento".

Autores da proposta: *Febraban.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 1º O titular pode opor-se a tratamento realizado com fundamento em uma das

hipóteses de dispensa de consentimento, comprovando o descumprimento ao disposto nesta Lei.

4.15.6. O exercício dos direitos do titular mediante seu requerimento a agentes de tratamento de dados pessoais

A principal crítica a esse parágrafo pelos participantes é em relação à obrigação de providências "imediatas". Segundo eles, não é factível e não encontra paralelo em leis nacionais ou estrangeiras a obrigação de prover imediatamente informações a pedido do titular de dados.

Sendo assim, os participantes pediram por prazos mais longos. O *US Business Council* requereu 30 dias; o *ITI,* 60 dias. Outros sugeriram que a futura lei determinasse que as providências deveriam ser tomadas em um "prazo razoável" (*Câmara BR, Brasscom, ABRANET, ABDTIC, Vivo* e *CNseg*). Dentre as contribuições cabe destacar a da *Brasscom* que, além de pedir um prazo razoável, também sugere critérios para definir este prazo. A *Fiesp* arguiu que o direito de acesso previsto neste parágrafo deve se limitar ao disposto no artigo 18, que traz a especificação do exercício deste direito.

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará providência para seu atendimento, nos termos do artigo 18 desta lei.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará providência para seu atendimento em prazo razoável, considerando-se a complexidade do pedido, bem como a da operação necessária para seu cumprimento em prazo razoável, considerando-se a complexidade do pedido bem como a da operação necessária para o seu cumprimento.

4.15.7. Casos de impossibilidade de cumprimento imediato de pedido relacionado a direito do titular do dados pessoais

Tal como no parágrafo anterior, boa parte das contribuições se concentrou na questão dos prazos. Nesse sentido, participantes do setor privado se manifestaram novamente contra a obrigação de prover "imediatamente" informações ao titular e, adicionalmente, pediram um prazo maior para o envio da resposta ao titular de que trata este parágrafo.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve impor ônus de comunicação ao titular caso seu pedido não possa ser imediatamente atendido.

"Este parágrafo deve ser excluído. Este parágrafo só acresce a carga burocrática imposta pela lei. Lei esta que já se apresenta extremamente detalhista, tratando muitas vezes de matéria que deveria ser abordado em regulamento ex post, ou seja, somente depois que se venha a perceber a necessidade da intervenção do Estado para corrigir distorções e práticas que possam colocar em risco a consecução dos objetivos da Lei.

Autores da proposta: *SindiTeleBrasil* e *Fiesp.*

(B) A comunicação ao titular de dados pessoais deve possivelmente conter quem é o agente de tratamento de dados pessoais, caso esse for o motivo da impossibilidade de atendimento ao seu pedido.

Autor da proposta: *ABDTIC.*

(C) O dever de comunicação deve facultar ao responsável pelo tratamento de dados pessoais a explicação dos motivos da impossibilidade de atendimento imediato do pedido do titular.

Autor da proposta: *ITI.*

(D) O responsável deve poder justificar de outras formas a impossibilidade de atendimento do pedido do titular.

Autor da proposta: *Brasscom.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[INCLUSÃO] III – justificar de outra forma a impossibilidade de atendimento do pedido;

4.15.8. Gratuidade no atendimento de pedidos relacionados a direitos dos titulares dos dados pessoais

Todos os participantes que comentaram este parágrafo sugeriram que alguns custos, desde que dentro do razoável e que não seja onerosos de maneira desproporcional, poderiam ser repassados ao titular.

Sugestões de redação:

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] § 4º a providência de que trata o parágrafo 2º será realizada sem ônus para o titular, sendo permitido cobrar apenas o custo normal de transmissão dos dados.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 4º A providência de que trata o § 2º será realizada sem ônus desproporcional para o titular.

4.15.9. Dever do responsável de informar a terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio

Propostas avulsas para a regulação deste tema:

(A) O dever do responsável de informar a terceiros a quem os dados tenham sido comunicados deve se limitar aos casos em que não seja "comprovadamente impossível" ou não implique "um esforço desproporcional".

"Sugerimos a retirada do parágrafo ou a nova redação abaixo apresentada, por ser mais um condicionante que, se mantido como publicado na Consulta Pública, poderá ser inviável de atendimento em função da possibilidade de não mais existir vínculo contratual ou comercial entre o responsável e terceiros". [*SindiTeleBrasil*]

"O dever de informar terceiros deve ser expressamente limitado às reais possibilidades do caso. 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". [*CNseg*]

Autores da proposta: *Brasscom, CNseg* e *SindiTeleBrasil.*

(B) A lei não deve instituir um dever do responsável de informar a terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio.

"Esta não é uma exigência adequada. Primeiramente, os titulares não gostariam que terceiros adotassem esses procedimentos com relação aos seus dados – portanto, o responsável não deve estar obrigado a informar os terceiros. Ainda, o responsável não poderá verificar se os terceiros adotaram

esses procedimentos".

Autor da proposta: *ITI.*

(C) A lei deve apenas instituir uma faculdade ao responsável de informar a terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio.

"Não deve haver obrigação de informar terceiros e sim uma faculdade. Isso porque será inviável, se não até impossível, comunicar sempre a todos que tiveram acesso aos dados. Essa obrigação deve ser limitada, como medida de razoabilidade e proporcionalidade".

Autor da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 5º Salvo as hipóteses em que a medida for comprovadamente impossível ou implicar em ônus desproporcionais. 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.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] O responsável deverá, sempre que possível, 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.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 5º Sempre que possível, o responsável deve informar os terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento.

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] § 5º O responsável poderá adotar sistemas de proteção e antifraude para verificar e garantir que o solicitante de confirmação, acesso, correção, dissociação, bloqueio ou cancelamento é o titular dos dados.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~17~~ 18. O titular dos dados pessoais tem direito a ~~obter:~~ obter, em relação aos seus dados:

I – confirmação da existência de ~~tratamento de seus dados;~~ tratamento**;**

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados; ~~e~~

IV – ~~dissociação~~ anonimização, bloqueio ou ~~cancelamento~~ eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta ~~Lei~~ Lei**;**

V – portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto;

VI – eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e

VII – aplicação das normas de defesa do consumidor, quando for o caso, na tutela da proteção de dados pessoais.

§ 1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, ~~alegando~~ em caso de descumprimento ao disposto nesta Lei.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2º, o responsável enviará ao titular, em até sete dias a partir da data do recebimento ~~da comunicação~~ do requerimento, resposta em que poderá:

I – a comunicar que não é agente de tratamento dos ~~dados;~~ dados, indicando, sempre que possível, quem o seja; ou

II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 4º A providência de que trata o § 2º será realizada sem ~~ônus~~ custos para o titular. **§ 5º** O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, ~~cancelamento~~

eliminação, ~~dissociação~~ anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

4.16. Exercício do direito de confirmação de existência ou acesso a dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.

§ 2º As informações e dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para tal fim; ou

II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º O titular poderá solicitar cópia eletrônica 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.

§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

Além das várias indagações sobre o significado da expressão "formato simplificado", a discussão concernente ao artigo 18 passou por três pontos principais. Em primeiro lugar, tal como no artigo anterior, a questão dos prazos foi levantada; mais especificamente, foi discutida a adequação dos prazos aos diferentes tipos de tratamento de dados. Em segundo lugar, foram trazidas sugestões de exclusão ou modificação do artigo, relacionadas a preocupações com a segurança jurídica. Por fim, houve o debate acerca dos formatos a serem utilizados para garantir o

acesso aos dados aos titulares. Neste ponto, como se verá, há uma divisão de opiniões entre aqueles que defendem maior flexibilidade no formato e aqueles que advogam pelo uso de dados abertos e inoperáveis.

4.16.1. Prazos para o exercício dos direitos de confirmação de existência ou de acesso a dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve adotar o critério da razoabilidade para a definição do prazo para atendimento de pedidos relacionados ao direito do titular dos dados pessoais.

Argumento que o tempo necessário para o cumprimento da obrigação disposta no artigo pode variar segundo características e circunstâncias diversas do tratamento de dados.

Autores da proposta: *Brasscom, ABDTIC, ABRANET, Câmara BR, Vivo, MPA* e *BSA.*

4.16.2. Propostas de exclusão ou modificação das definições para exercício dos direitos e confirmação de existência ou acesso a dados pessoais

Propostas avulsas para a regulação deste tema:

(A) As disposições para o exercício de tais direitos já estão previstas no Código de Defesa do Consumidor.

Autor da proposta: *Claro.*

(B) As disposições para o exercício de tais direitos devem ser previstas em sede de regulamentação.

Autor da proposta: *SindiTeleBrasil.*

(A) O pedido de acesso a dados pessoais deve ser condicionado à solicitação formal do titular junto ao encarregado.

Autor da proposta: *Fiesp.*

4.16.3. Como a lei deve abordar a questão do formato dos dados a serem disponibilizados aos seus titulares, mediante o seu requerimento?

Respostas controversas coletadas na plataforma de debate:

(A) A lei não deve prescrever formatos específicos.

"*A definição em Lei de formatos específicos, ou mesmo a possibilidade de um órgão competente predeterminá-los, pode ser prejudicial ao ambiente de tratamento de dados, uma vez que entes das mais diversas naturezas exercem tais atividades. A diretiva europeia, por exemplo, apenas prescreve a 'comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados'*". [*Brasscom*]

Quem defendeu isso? *Brasscom* e *ITI.*

(B) A lei deve garantir ao titular dos dados pessoais que o formato de disponibilização seja "interoperável".

"Este artigo dispõe sobre o direito de portabilidade do titular com relação aos seus dados. Neste ponto, o anteprojeto brasileiro parece ser ainda mais protetivo do que o sistema europeu (não há as limitações quanto ao formato 'comumente utilizado' ou a necessidade de um contrato entre responsável e titular presentes no sistema europeu), no entanto, parece importante estabelecer expressamente que o direito a portabilidade é estabelecido sem prejuízo da necessidade de exclusão de dados quando não mais necessários. Além disso, nos parece importante aperfeiçoar a redação do artigo de forma a estabelecer o direito a obter cópia interoperável, e que tal interoperabilidade pode ser realizada mais eficazmente através do uso de formatos abertos.

Por fim, há de se estabelecer critérios mais específicos para a garantia do direito a portabilidade, equilibrando esse direito com o correspondente ônus gerado aos diferentes responsáveis por tratamento de dados, de forma a evitar obrigações excessivas".

Quem defendeu isso? *CTS-FGV.*

Propostas avulsas para a regulação deste tema:

(A) A lei deve limitar o direito de acesso do titular de dados pessoais para que não haja revelação de segredos de negócio do responsável.

"Inciso II deve fazer uma ressalva com relação aos segredos empresariais do responsável. Isso porque o responsável não poderá informar ao titular os critérios de utilização dos dados pessoais, por serem essas informações segredos das entidades que, se divulgados, podem gerar graves prejuízos ao negócio.

Destacamos que o legislador, quando a edição da Lei n.º 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, pensando nesse cenário, fez acertadamente no artigo 5º, inciso IV, a ressalva aos segredos empresariais quando previu que o titular dos dados constantes no cadastro de Histórico de Crédito pode obter informações a respeito dos principais elementos e critérios considerados para a análise do risco de crédito".

Autor da proposta: *Febraban.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular, mediante solicitação formal ao encarregado.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 18. O acesso a dados pessoais será providenciado em formato inteligível e dentro de prazo razoável, a contar do recebimento da solicitação do titular pelo responsável.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] II- por meio de declaração clara e completa, que indique a origem dos dados, data de registro e finalidade do tratamento, ressalvados os segredos empresariais, fornecida no prazo de até sete dias úteis, a contar do momento do requerimento do titular;

4.16.4. Meio de disponibilização de informações e dados requeridos pelo titular dos dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer como regra geral a disponibilização de informações e dados por meio eletrônico.

"O artigo 18 confere ao titular dos dados a capacidade de escolher entre receber as informações solicitadas de forma eletrônica ou em cópia física ("formato impresso"). Para que o processador dos dados forneça as informações solicitadas de maneira eficiente e sem ônus excessivo, o artigo 18 deveria ser alterado para determinar que o formato eletrônico deve ser o formato padrão. O fornecimento em qualquer outro formato, incluindo cópia física, deve ser uma exceção apenas caso o titular dos dados declare a impossibilidade de acessar as informações por via eletrônica".

Autor da proposta: *BSA.*

(B) A disponibilização de informações e dados por forma impressa não deve criar ônus financeiro para titulares que sejam comprovadamente hipossuficientes.

"No caso de informações recebidas por forma impressa, sugere-se a inclusão de uma exceção ao pagamento pelo titular por informações recebidas desde que comprovada hipossuficiência financeira".

Autor da proposta: *Jhonata Goulart Serafim.*

Sugestões de redação:

Autor da sugestão: *BSA.*

[MODIFICAÇÃO] § 2º As informações e dados serão fornecidos, por meio eletrônico, seguro e idôneo.

I – Em casos excepcionais, a informação poderá ser fornecida de forma impressa, somente se o titular dos dados declarar a impossibilidade de acesso à informação por meio eletrônico. Nestes casos, poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados;

4.16.5. Controvérsia sobre a possibilidade de o órgão competente dispor sobre os formatos em que serão fornecidas as informações e os dados aos titulares

A divergência entre os participantes do setor privado que discordaram sobre a possibilidade de o órgão competente de dispor sobre os formatos em que serão fornecidas informações e dados aos titulares se deu com relação a quem deve determinar este formato: o responsável pelo tratamento ou o titular dos dados.

Respostas controversas coletadas na plataforma de debate:

(A) O responsável pelo tratamento deve poder determinar o formato de disponibilização de informações e dados.

"*Sugerimos a remoção do parágrafo 4º do art. 18, uma vez que a definição da melhor forma deve ser dada pelo responsável pelo tratamento, de acordo com as circunstâncias, desde que permita ao titular a efetiva compreensão da informação requerida*" [*Vivo*].

Quem defendeu isso? *Câmara BR, Brasscom, Vivo, ABDTIC e ABRANET*.

(B) O titular dos dados deve poder determinar o formato de disponibilização de informações e dados.

"Sugerimos que o parágrafo seja suprimido. O artigo 18 do Anteprojeto já prevê que caberá ao próprio titular escolher qual a forma de recebimento das informações e dados. Caberá, portanto, ao titular escolher o formato que melhor se adeque às suas necessidades".

Quem defendeu isso? *Febraban.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~18~~ 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a ~~contarem do momento~~ contar da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que ~~permita~~ favoreça o exercício do direito de acesso.

§ 2º As informações e dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para tal fim; ou

II – sob ~~a~~ forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados. **§ 3º** ~~O~~ Quando o tratamento tiver origem no consentimento do titular ou em um contrato, o titular poderá solicitar cópia eletrônica 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~~.

§ 4º ~~Órgão~~ O órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

§ 5º O órgão competente poderá dispor de forma diferenciada acerca dos prazos dos incisos I e II do caput para setores específicos**.**

4.17. Direito de revisão de decisões tomadas com base no tratamento automatizado de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.

§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal.

Propostas avulsas para a regulação deste tema:

(A) O direito de revisão de decisões tomadas com base no tratamento automatizado de dados pessoais deve ser limitado a decisões que tenha impacto "em determinados aspectos da personalidade do titular", como capacidade profissional e confiança.

"O direito de revisão deverá estar limitado às áreas especializadas nas quais a decisão resulte em um impacto significativamente adverso sobre o seguinte: disponibilidade de crédito, termos de seguro, emprego ou moradia.

Além do mais, o direito de revisão não deve estar condicionado a forma (automatizada ou não) com que a decisão que afeta interesses seja tomada". [*ITI*]

Autores da proposta: *Brasscom* e *ITI.*

(B) A lei não deve criar um direito de revisão de decisões tomadas com base no tratamento automatizado de dados pessoais.

"Sugere-se exclusão do artigo. Este artigo estabelece mais um condicionante que estabelece obrigação operacional ao responsável e que é bastante discutível. O responsável deve ter o diretivo e a liberdade de avaliar os resultados do tratamento dos dados pessoais do titular, para seu uso interno, da forma como ele julgar mais adequada para si e para a destinação e finalidade que o tratamento dos dados tem". [*Claro*]

"Sugere-se a eliminação do artigo, já que nele se verifica uma ingerência na tomada de decisão das empresas sempre que, por exemplo, alguma decisão de não contratação seja adotada, pelo fato de o cliente ter um histórico de fraude na empresa. Há, portanto, prejuízo a liberdade de contratar e de escolher o conteúdo do contrato, tal como disposto no CC, artigo 421". [*Vivo*]

Autores da proposta: *Claro* e *Vivo.*

(C) O direito de revisão de decisões tomadas com base no tratamento automatizado de

dados pessoais deve se limitar aos casos que forem tornados públicos.

"A definição de perfil, avaliação de aspectos de sua personalidade, classificação, enquadramento, conclusão ou resultado advindo do tratamento dos seus dados que não forem tornadas públicas, nem transferidas a terceiros não estão sujeitas a revisão".

Autores da proposta: *SindiTeleBrasil.*

(D) A lei deve estipular um prazo legal para resposta de pedido do titular com base no direito de revisão de decisões tomadas com base no tratamento automatizado de dados.

"Necessária a previsão de prazo para que o pedido de revisão seja respondido. É importante que se estabeleça prazo para que a revisão seja respondida, sob pena de multa; caso contrário, tal direito em questão pode se tornar inócuo".

Autores da proposta: *Priscila M.*

(E) A lei deve criar uma exceção ao direito de revisão de decisões tomadas com base no tratamento automatizado de dados para fins pesquisas de mercado.

"Acreditamos que pesquisas de mercado não causam prejuízos ao titular dos dados, posto que só tratam de dados anônimos e não individualizados, daí não ser adequada a permissão de que solicitem a revisão de quaisquer decisões tomadas.

Não pode haver prejuízo ao titular dos dados caso esses sejam utilizados exclusivamente para Pesquisas de Mercado, tipicamente com resultados anônimos e não individualizados. Por isso, não parece adequada a permissão de que solicitem a revisão de quaisquer decisões tomadas".

Autor da proposta: *ABEP.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas com base em tratamento automatizado de dados pessoais que adversamente afetem seus interesses relacionados à sua capacidade profissional, financeira, creditícia e de moradia.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 19. O titular dos dados pessoais tem o direito de solicitar a revisão de qualquer tipo de definição de perfil, avaliação de aspectos de sua personalidade, classificação, enquadramento, conclusão ou resultado advindo do tratamento dos seus dados, sempre que forem tornadas públicas ou transferidas a terceiros.

Autor da sugestão: *ABEP.*

[INCLUSÃO] §3º Ficam dispensadas das obrigações previstas neste artigo empresas que coletem os dados sem a finalidade de orientar decisões específicas ao titular dos dados, a título de subsídio para análises estatísticas e pesquisas de mercado.

4.17.1. Fornecimento de informações adequadas sobre decisões tomadas com base no tratamento automatizado de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever que o fornecimento de informações adequadas sobre decisões tomadas com base no tratamento automatizado de dados pessoais deva respeitar segredos de comércio e indústria.

Segundo os participantes que defenderam esta posição, a redação posta para debate público violaria a proteção de segredos de indústria, de comércio e de negócio. O dispositivo ainda facilitaria fraudes contra seguros, já que seria mais fácil conhecer os critérios e procedimentos utilizados pelas seguradoras e, assim, encontrar caminhos para burlar sistemas de aceitação.

Autores da proposta: *Febraban, ABA, Câmera BR, Fiesp, CNseg* e *ABDTIC.*

(B) A lei deve prever que o fornecimento de informações adequadas sobre decisões tomadas com base no tratamento automatizado de dados pessoais possa ser realizado através da revelação das categorias dos critérios utilizados no tratamento.

Autor da proposta: *ITI.*

(A) A lei não deve prever o fornecimento de informações adequadas sobre decisões tomadas com base no tratamento automatizado de dados pessoais.

"Adicionalmente à argumentação exposta na sugestão acerca da eliminação do caput deste artigo, sugere-se que também o parágrafo primeiro seja retirado. Pois esta norma constituir uma violação dos incisos XI e XII do Artigo 195 da Lei n.º 9279 de 14 de Maio de 1996 (que regula direitos e obrigações relativos à propriedade industrial), os quais conferem proteção aos dados confidenciais ou informações das empresas. Tal como está, a redação consiste em uma ameaça a proteção de dados confidenciais dos responsáveis, os quais já gozam de proteção jurídica na lei brasileira".

Autor da proposta: *Vivo.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada, resguardado o segredo empresarial.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada, ressalvados os segredos de negócios estabelecidos contratualmente ou em legislação específica.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] §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.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~19~~ 20. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

~~§ 1º~~ **Parágrafo único.** O responsável deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada~~.~~

~~§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal~~, respeitado o segredo comercial e industrial.

4.18. Vedação ao uso de dados pessoais referentes a exercício regular de direitos pelo titular em seu prejuízo

REDAÇÃO LEVADA A DEBATE

Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo

Propostas avulsas para a regulação deste tema:

(A). A lei não deve criar uma vedação ao uso de dados pessoais em prejuízo do titular voltada a dados obtidos legalmente.

"O disposto no art. 20, que veda o uso de dados em prejuízo do titular, quando referentes ao exercício regular de direitos, é bastante vago e, por isso, permite interpretações imprecisas. Ao praticar atividades financeiras, por exemplo, o cidadão exerce regularmente seus direitos. No entanto, isso não deveria impedir uma instituição bancária de, com base em tais dados, definir um limite de crédito para o titular dos dados" [*Brasscom*]

"Sugere-se a eliminação do artigo. Tal como o artigo 19, este artigo dispõe sobre uma ingerência desproporcional do estado nas relações contratuais e lesão ao direito de liberdade de contratar". [*Vivo*]

Autores da proposta: *Brasscom, Vivo* e *ABDTIC.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~20~~ 21. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

4.19. Tutela coletiva dos direitos dos titulares dos dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 21. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei nº 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei nº 8.078, de 11 de setembro de 1990, na Lei nº 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

Propostas avulsas para a regulação deste tema:

(A). Caso a lei crie um órgão federal para regular a aplicação das normas referentes ao tratamento de dados pessoais suas interpretações devem servir para uniformizar o

entendimento judicial.

"A descentralização excessiva do processo de análise técnica, bem como de interpretação e aplicação desta Lei pode gerar insegurança jurídica para as empresas que precisem realizar o tratamento de dados como parte das suas atividades, prejudicando a competitividade do país".

Autor da proposta: *Brasscom.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~21~~ 22. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei nº 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei nº 8.078, de 11 de setembro de 1990, na Lei nº 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

4.20. Responsabilidade solidária nos casos de comunicação e interconexão de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.

4.20.1. Como deve se dar a distribuição da responsabilidade nos casos de comunicação ou interconexão? A responsabilidade solidária se justifica?

Respostas controversas coletadas na plataforma de debate:

(A) Responsabilidade exclusiva do cedente[24].

"A responsabilidade solidária resulta em um desestímulo enorme aos negócios de processamento e outsourcing de dados, pois gera confusão entre os papéis desempenhados pelo responsável e pelo operador – que muitas vezes equivalem ao cedente e cessionário nesse tipo de contratação. Se o Brasil quer desenvolver o mercado de serviços nessa área, é importante que se delimite as regras aplicáveis a um e outro, afastando-se do modelo de solidariedade". [*ABRANET*]

"*A responsabilidade solidária entre responsável (cessionário) e processador (cedente) de dados da forma como proposta no anteprojeto de Lei poderá levar a uma responsabilização indevida dos agentes envolvidos na operação de tratamento. Qualquer agente que estiver processando informações pessoais já está sujeito à obrigação de respeitar a Lei, mas a responsabilidade solidária, como tratada neste artigo, pode não ser compatível com as funções e os atos efetivos das partes. É importante distinguir bem tais funções e atos, pois é com base nessa distinção que devem ser atribuídos os deveres e responsabilidades de cada um desses agentes, conforme princípio abraçado pelo Código Civil brasileiro, art. 927*". [*Brasscom*]

Quem defendeu isso? *Câmara BR, Brasscom, Febraban, US Business Council, ABRANET, ABINEE, CNI* e *CNseg*.

(B) Responsabilidade exclusiva do responsável pelo tratamento.

"*A responsabilização solidária cria incertezas quanto ao real responsável por eventuais danos ou irregularidades, e o operador poderá ser responsabilizado por perdas e danos que não guardam relação com o tratamento que realiza. Além disso, o Responsável é a figura mais provável pela interação com o titular, o que, portanto, tornaria mais complicado para o usuário quando fosse necessário ingressar com qualquer medida judicial para reparação danos ou pleitear indenizações"*. [*Cisco*]

Quem defendeu isso? *Cisco e BSA.*

(C) Responsabilidade solidária entre cedente e cessionário, apenas quando cessionário não for localizado ou identificado.

"*A responsabilidade solidária entre cedente e cessionário deve estar atrelada a finalidade da cessão e só deve ocorrer caso não seja possível localizar ou identificar o cessionário. Isso porque a solidariedade entre estes agentes nem sempre se justificará na medida em que o cedente, muitas vezes, terá atuação diminuta e até inexpressiva no tratamento e, além disso, o cedente sofrerá com altos e injustificados custos para fiscalizar a atuação do cessionário*".

Quem defendeu isso? *ABEMD*.

(D) Responsabilidade exclusiva do agente realizador da coleta.

"Sugerimos a supressão deste artigo e de seu parágrafo único. No contexto da comunicação e

[24] Os participantes que defendem esta posição sugeriram, em sua maioria, a supressão do dispositivo no texto legal.

interconexão de dados, a solidariedade se apresenta como um fardo excessivo que acabará por aumentar os preços dos produtos e serviços por eles ofertados e eventualmente será prejudicial para negócios no Brasil. O agente realizador da coleta é quem está na melhor posição para evitar danos aos usuários".

Quem defendeu isso? *MPA*.

(E) Responsabilidade do cessionário baseada no nível de auditoria conduzida pelo cedente.

"A responsabilidade do cessionário deverá se basear no nível de auditoria conduzida pelo cedente. A responsabilidade solidária não seria apropriada se o cedente tiver adotado as medidas apropriadas para assegurar o devido tratamento das informações pelo cessionário".

Quem defendeu isso? *ITI*.

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente.

4.20.2. Exceções ao regime de responsabilidade solidária na comunicação ou interconexão de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever uma exceção ao regime de responsabilidade solidária na comunicação ou intercomunicação de dados pessoais para fins de pesquisas de mercado, históricas e científicas.

"Alterações devem ser feitas para incluir as pesquisas de mercado, pesquisas históricas e pesquisas científicas na categoria em que não haverá responsabilidade solidária entre o cessionário e o cedente a exemplo dos casos em que a interconexão é realizada em exercício dos deveres impostos pela Lei de Acesso à Informação.

Só assim estará garantido o pleno exercício das atividades de pesquisa que, mesmo em casos de interconexão, garantem o anonimato das informações perante terceiros".

Autor da proposta: *ABEP.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~22~~ 23. ~~Nos casos de comunicação ou interconexão~~ O tratamento de dados pessoais~~, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados. Parágrafo único. A responsabilidade solidária não se aplica aos casos~~ pelas pessoas jurídicas de ~~comunicação ou interconexão realizadas~~ direito público referenciadas no ~~exercício dos deveres de que trata a~~ parágrafo único do art. 1º da Lei ~~no~~ 12.527, de 18 de novembro de 2011, ~~relativos à garantia do acesso~~ deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a ~~informações públicas~~ execução de competências legais ou o cumprimento de atribuição legal pelo serviço público.

4.21. Consentimento para comunicação ou interconexão de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

4.21.1. Como deve se dar a autorização para a comunicação e interconexão de dados? O consentimento livre, expresso, específico e informado deverá ser usado para todos os casos?

Propostas avulsas para a regulação deste tema:

(A) Deve ser eliminada a exigência de consentimento.

Segundo os defensores desta posição "o armazenamento de um grande volume de dados deve ser feito através de programas em nuvem com servidores, muitas vezes, hospedados no exterior". Assim, nesse contexto, as interconexões seriam constantes "e não seria factível pedir um consentimento para cada uma delas". A solução seria "requisitar uma autorização prévia e abrangente, embora pormenorizada o suficiente para proteger direitos dos titulares de dados".

Claro, SindiTeleBrasil e *GSMA* sugerem que o artigo seja excluído. Segundo elas "o art. 10º já deixa claro que no momento do consentimento o usuário deve ser informado sobre sujeitos ou categorias de sujeitos para os quais os dados podem ser divulgados ou fornecidos a terceiros".

Autores da proposta: *ABEP*, *Claro, SindiTeleBrasil e GSMA*.

(B) Deve haver exigência de consentimento, mas ele não precisa ser "expresso e específico".

A comunicação de dados pessoais entre pessoas de direito privado deve depender do consentimento livre e informado, mas não necessariamente expresso e específico dos titulares. Isso porque a necessidade de consentimento expresso e específico acaba por gerar grandes custos para as empresas e pode acarretar "fadiga de consentimento" por parte dos titulares. Para evitar esses malefícios, sugere-se partir de uma abordagem baseada nas cláusulas contratuais entre os agentes, autorizando a comunicação e aplicação de medidas para garantir que os titulares tenham exata ciência e controle da comunicação dos seus dados.

Autor da proposta: *Brasscom e Febraban.*

(C) Deve haver uma exceção ao consentimento que permita a livre comunicação de dados ou interconexão de dados entre empresas do mesmo grupo econômico, conglomerado multinacional ou parceiros.

"Sugerimos que seja incluída uma alternativa para este dispositivo, no sentido de se prever que entre empresas do mesmo grupo econômico, conglomerado multinacional ou parceiros não deverá haver restrições à comunicação de dados ou à interconexão de dados".

Autor da proposta: *Vivo*.

(D) Deve haver uma exceção à exigência de consentimento para interconexão de dados para fins estatísticos, acadêmicos ou de pesquisa.

"Sugerimos que o Anteprojeto, com o objetivo de não prejudicar a conservação de registros históricos, bem como facilitar a transferência de dados entre institutos de pesquisa, tenha dispositivo expresso autorizando a comunicação ou interconexão de dados pessoais entre pessoas de direito privado sem o consentimento do titular para fins estatísticos, acadêmicos ou de pesquisa, nos casos em que não é possível obter o consentimento do titular tal como já ocorre na legislação canadense".

Autor da proposta: *Associação da Liberdade Religiosa e Negócios*.

(E) A lei deve prever uma possibilidade de revogação do consentimento nestes casos.

Diante da necessidade de consentimento, também deve haver a possibilidade de revogação deste consentimento, preferencialmente a qualquer tempo e através de canal de fácil acesso.

Autor da proposta: *Daniel Astone*.

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 23. A comunicação ou interconexão de dados pessoais é permitida entre pessoas jurídicas de direito privado com sede no Brasil que pertençam ao mesmo grupo econômico, sem necessidade de consentimento específico, desde que todas as pessoas jurídicas mantenham os mesmos padrões e políticas de proteção de dados pessoais.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 23. A comunicação de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~23~~ 24. ~~A comunicação ou interconexão~~ Os órgãos do Poder Público darão publicidade às suas atividades de tratamento de dados pessoais ~~entre~~ por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no art. 5º, VI desta Lei.

§ 1º Os órgãos do Poder Público que realizem operações de tratamento de dados pessoais deverão indicar um encarregado, nos termos do art. 40.

§ 2º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

Art. 25. As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado ~~dependerá~~ particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e sociedades de ~~consentimento livre~~ economia mista, ~~expresso~~ quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, ~~específico~~ terão o mesmo tratamento dispensado aos órgãos e ~~informado~~ entidades do Poder Público, ~~ressalvadas as hipóteses~~ nos termos desse Capítulo.

Art. 26. O uso compartilhado de ~~dispensa do consentimento previstas nesta~~ dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.

Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observado, ainda, o disposto na Lei nº 12.527, de 18 de novembro de 2011.

4.22. Comunicação ou interconexão de dados pessoas em pessoas de direito público e privado

REDAÇÃO LEVADA A DEBATE

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

I – nas hipóteses de dispensa do consentimento previstas nesta Lei;

II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou

III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.

Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:

I – à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;

II – ao oferecimento aos titulares de opção de cancelamento de seus dados; ou

III – ao cumprimento de obrigações complementares determinadas por órgão competente.

4.22.1. Como deve se dar a autorização de comunicações e interconexões de dados pessoais entre pessoas jurídicas de direito pública e pessoas de direito privado?

Nesse ponto de debate notou-se uma preocupação do setor privado em relação a um suposto desequilíbrio de tratamento entre pessoas jurídicas de direito público e de direito privado. Argumentos transitaram entre a imposição de ônus excessivo e a preocupação com a privacidade dos titulares de dados pessoas frente ao poder do Estado.

Respostas controversas coletadas na plataforma de debate:
(A) A lei deve condicionar a comunicação ou interconexão de dados pessoais entre pessoas jurídicas de direito público e de direito privado à prévia autorização do poder legislativo. O anteprojeto deve condicionar a coleta de dados pessoais por órgãos públicos à prévia autorização do poder legislativo, ou seja, via projeto de lei, em que se especifique que os dados serão coletados, sua finalidade, quem poderá acessá-los e tratá-los e os prazos para manutenção de tais dados em arquivo. **Quem defendeu isso?** *Rodrigo Veleda*
(B) A lei deve condicionar a comunicação ou interconexão de dados pessoais entre pessoas jurídicas de direito público e de direito privado ao consentimento do titular em todos os casos. Para os defensores desta posição, os incisos do artigo devem ser suprimidos para que não exista exceção à necessidade de consentimento. Todas as comunicações e interconexões deveriam, portanto, depender do consentimento do titular, não devem haver exceções. Até mesmo diante das hipóteses do APL em que o consentimento para a coleta é dispensado, se houver posterior comunicação ou interconexão da dados deverá haver consentimento do usuário. Isso porque

operações de comunicação e interconexão são consideravelmente de maior risco (citou-se o episódio do acordo entre o TSE e a SERASA[25]).

Quem defendeu isso? *Proteste, Luiz Perin Filho, Joana Varon* e *GPoPAI.*

(C) A lei deve condicionar a comunicação ou interconexão de dados pessoais entre pessoas jurídicas de direito público e de direito privado ao consentimento do titular em todos os casos, exceto os de obrigação legal ou de cumprimento de ordem judicial.

Quem defendeu isso? *Veridiana/Intervozes*.

(D) A lei deve condicionar a comunicação ou interconexão de dados pessoais entre pessoas jurídicas de direito público e de direito privado ao consentimento livre e informado, mas não necessariamente expresso, dos titulares.

Quem defendeu isso? *Brasscom e Febraban*.

(E) A lei deve condicionar a comunicação ou interconexão de dados pessoais entre pessoas jurídicas de direito público e de direito privado ao consentimento do titular em todos os casos.

"Sugerimos alteração do artigo de forma a criar um procedimento que terá como finalidade denifir (sic) as hipóteses em que a comunicação ou interconexão de dados será permitida sem o consentimento livre, expresso, específico e informado".

Quem defendeu isso? *GPoPAI*.

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar um regime único para pessoas jurídicas de direito público e de direito privado sujeito à necessidade de consentimento livre, expresso, específico e informado do titular.

Autores da proposta: *Claro, Vivo, SindiTeleBrasil* e *GSMA.*

(B) A lei deve ser mais rigorosa em relação ao compartilhamento de dados entre os órgãos públicos.

"Este inciso (art. 24, II) *reflete uma permissividade excessiva do compartilhamento de dados entre os órgãos públicos. Há visível desequilíbrio entre as obrigações impostas ao setor público e ao setor privado que resulta em uma maior vulnerabilidade do cidadão perante o estado. A dispensa deverá ser melhor especificada para garantir os direitos dos usuários.*

Ademais, haverá casos em que, por exemplo, o tratamento será conjunto, entre entes públicos e

[25] Em 2013 o Tribunal Superior Eleitoral envolveu-se em polêmica por conta de convênio com a SERASA, empresa privada. Fonte: http://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255

privados, inviabilizando a dualidade de regimes".

Autores da proposta: *ABRANET* e *ABDTIC.*

(C) A lei não deve conter uma dispensa de consentimento para o compartilhamento ou interconexão de dados pessoas entre pessoas jurídicas de direito público e direito privada quando houver prévia autorização do órgão competente.

"Sugerimos a eliminação do inciso. Dispositivo concede um elevado grau de discricionariedade ao órgão público. Interconexão só dependerá do consentimento de titular e não deverá ficar na dependência do "órgão competente" a possibilidade de se proceder à interconexão de dados" (*GSMA*).

"*O inciso deixa grande margem de discricionariedade à autoridade regulador, permitindo a ele avaliar exceções de interesse público. Deve-se, portanto, tomar especial cuidado com a composição, poderes e natureza dessa autoridade"* (*ABDTIC*).

Autores da proposta: *GSMA, Vivo* e *ABDTIC.*

(D) A lei deve prever que a dispensa de consentimento, autorizada por órgão competente para comunicação ou interconexão de dados pessoais entre pessoas de direito público e direito privado, deve ser restrita a uma autoridade de proteção de dados pessoais e não a qualquer outro órgão.

"Este avaliará as solicitações de dispensa encaminhadas por outros órgão públicos".

Autor da proposta: *GEPI-FGV.*

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado e entre as próprias pessoas jurídicas e órgãos públicos sem o consentimento livre, expresso, específico e informado do titular, só será admitido mediante o seguinte procedimento:

§ 1º A pessoa jurídica de direito público interessada na interconexão ou comunicação de dados pessoais deve fazer solicitação formal ao órgão competente;

§ 2º A solicitação deve ser circunstanciada, explicando a necessidade de interconexão e comunicação, comprovando-se:

a. a necessidade do tratamento dos dados para o cumprimento eficaz de uma finalidade dentro da sua competência;

b. a impossibilidade de atender de maneira eficaz esta finalidade por outros meios que dispensem o tratamento de dados pessoais, em particular se forem sensíveis;

c. que solicita o tratamento da menor quantidade de dados necessária para atender eficazmente a

finalidade especificada;

d. que os dados sejam, sempre que possível, anonimizados, de acordo com as obrigações previstas no art. 11, inciso VII, justificando-se, de forma circunstanciada, a sua impossibilidade e/ou a adoção de outras medidas de segurança.

§ 3º O órgão competente julgará a adequação da solicitação mediante a análise dos princípios dispostos nessa legislação, atendendo-a parcialmente ou totalmente, bem como estabelecendo o período de validade para a autorização, os procedimento para cancelamento posterior e medidas de segurança aplicáveis;

§ 4º Uma vez autorizado o estabelecimento de uma comunicação ou interconexão dos dados pessoais, tal decisão, com as razões que a embasaram, deve ser publicizada pelo órgão competente;

§ 5º Os legitimados para ações coletivas e ação civil pública poderão recorrer da decisão do órgão competente que poderá rever decisão anterior com base na avaliação de novos elementos providos por essas entidades.

Autor da sugestão: *Veridiana/Intervozes.*

[MODIFICAÇÃO] Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo por obrigação legal que as determine.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado e entre pessoas de direito público entre si ou entre pessoas de direito privado entre si dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 24.A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre e informado do titular, salvo:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado e entre pessoas de direito público entre si ou entre pessoas de direito privado entre si dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 24. A comunicação de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre e informado do titular,

salvo:

[SUPRESSÃO] Parágrafo único e incisos.

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] Art. 24.A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado e entre pessoas de direito público entre si ou entre pessoas de direito privado entre si dependerá de consentimento livre, específico e informado do titular, salvo:

Autor da sugestão: *RELX Group.*

[MODIFICAÇÃO] I - Nas hipóteses de dispensa do consentimento previstas na Lei 12.527, de 18 de novembro de 2011, no Artigo 31, Parágrafo 1, inciso II e Parágrafo 3, incisos I, II, III, IV e V;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~24~~ 27. A comunicação ~~ou interconexão~~ e transferência de dados pessoais ~~entre~~ de pessoa jurídica de direito público ~~e~~ a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento ~~livre, expresso, específico e informado~~ do titular, salvo:

I – nas hipóteses de dispensa do consentimento previstas nesta Lei; **ou:**

II – nos casos de uso compartilhado de dados ~~previsto no inciso XVII do art. 5º~~, em que será dada publicidade nos termos do art. 24 ~~§1º do art. 6º; ou III. quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.~~

~~Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:~~

~~I. à comunicação da interconexão aos titulares, nos termos do §1º do~~ art. ~~6º;~~

~~II. ao oferecimento aos titulares de opção de cancelamento de seus dados; ou~~

~~III. ao cumprimento de obrigações complementares determinadas por órgão competente~~

4.23. O dever de publicidade na comunicação ou interconexão de dados pessoais entre órgãos e entidades de direito público

REDAÇÃO LEVADA A DEBATE

Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve criar regime diferenciado para o tratamento de pessoas jurídicas de direito público.

Autores da proposta: *Claro e SindiTeleBrasil.*

(B) A lei deve determinar obrigações específicas de clareza, precisão e atualização das informações sobre tratamento de dados pessoais por órgãos e entidades de direito público.

Autor da proposta: *GPoPAI.*

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] Art. 25. Os órgãos e entidades de direito público darão publicidade às suas atividades de tratamento de dados pessoais por meio de informações claras, precisas e atualizadas em veículo de fácil acesso, preferencialmente em seus sítios eletrônicos.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~25~~ 28. A comunicação ~~ou interconexão~~ de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos ~~do §1º do~~ art. ~~6º, e obedecerá às regras gerais deste Capítulo~~ 24.

4.24. Comunicação e interconexão de dados pessoais: poderes do órgão competente

4.24.1. Poderes relacionados à comunicação e interconexão de dados pessoais de órgãos e entidades públicas

REDAÇÃO LEVADA A DEBATE

Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.

Propostas avulsas para a regulação deste tema:
(A) A lei não deve conferir um poder de recomendação ao órgão competente, sob pena de abrir espaço para insegurança jurídica e incerteza ao ambiente de negócios. **Autores da proposta**: *Brasscom* e *Vivo*[26].
(B) A lei deve instituir que as solicitações do órgão competente respeitem o direito de confidencialidade quanto a segredos empresariais. **Autor da proposta**: *Brasscom.*
(C) A lei não deve criar regime diferenciado para o tratamento de pessoas jurídicas de direito público, portanto não deve criar poderes específicos relacionados a elas. **Autor da proposta**: *Claro.*
(D) A lei deve permitir que solicitações sejam realizadas mesmo após a concessão de

[26] Vivo pede a retirada total do artigo.

autorização pelo órgão competente para comunicação ou interconexão.

Autor da proposta: *GPoPAI.*

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] Art. 26 O órgão competente poderá solicitar, a qualquer momento e mesmo após a concessão da autorização prevista no art. 24, aos órgãos e entidades [...].

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, ressalvado, quando aplicável, o direito do responsável ao segredo de negócio.

Autor da sugestão: *Jorge Machado.*

[MODIFICAÇÃO] Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizam (...)

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~26~~ 29. O órgão competente poderá solicitar, a qualquer momento, ~~aos órgãos e~~ às entidades ~~públicos~~ do Poder Público que realizem ~~interconexão~~ operações de ~~dados e o uso compartilhado~~ tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir ~~recomendações complementares~~ parecer técnico complementar para garantir o cumprimento desta Lei.

4.24.2. Poder normativo complementar do órgão competente para atividades de comunicação e interconexão de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.

Propostas avulsas para a regulação deste tema:

(A) A lei deve restringir os poderes normativos do órgão competente.

"Sugerimos a eliminação do artigo. Em respeito ao princípio da legalidade, o órgão competente será responsável pela interpretação ou edição dos atos interpretativos a respeito das regras existentes, dentro dos limites e do alcance estipulados em Lei" (*Brasscom*)

"Sugerimos a retirada do artigo. Para que a Lei possa efetivamente cumprir seu objetivo, o marco regulatório não deve criar distinção no tratamento das pessoas jurídicas de direito público e das pessoas jurídicas de direito privado. Não deve, portanto, haver diferença da necessidade de consentimento livre, expresso, específico e informado consoante se trate de comunicação ou interconexão entre as pessoas jurídicas de direito público ou pessoas jurídicas de direito privado". (*Claro*)

Autores da proposta: *Câmara BR, Vivo, Claro, Brasscom, ABDTIC* e *MPA*[27].

(B) A lei deve prever que a criação de novas normas deve estar submetida a processos de consulta pública, permitindo o envolvimento dos setores na sua elaboração.

Autor da proposta: *ITI.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais, de acordo com os limites e princípios previstos na presente lei.

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] Art. 27. É vedado aos órgãos públicos e entidades públicas efetuar a

[27] Vivo, Claro, Brasscom, ABDTIC e MPA pedem a retirada do artigo

transferência de dados pessoais constantes de base de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto os casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~27~~. 30. ~~Órgão~~ O órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.

Seção II – Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Parágrafo único. As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei nº 8.112, de 11 de dezembro de 1990, e na Lei nº 8.429, de 2 de junho de 1992.

Art. 32. O órgão competente poderá solicitar a agentes do poder público que publiquem relatórios de impacto de privacidade e sugerir adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

4.25. Transferência internacional de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:

I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

III – quando órgão competente autorizar a transferência, nos termos de regulamento;

IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.

Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:

I – normas gerais e setoriais da legislação em vigor no país de destino;

II – natureza dos dados;

III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV – adoção de medidas de segurança previstas em regulamento; e

V – outras circunstâncias específicas relativas à transferência.

O eixo de discussão a respeito das transferências internacionais foi um dos mais controversos na plataforma. Em meio ao debate, pouco consenso foi formado. Isso se deu, inclusive, pelo fato de que entre os participantes não houve sequer uma interpretação única sobre o que a redação original do anteprojeto procura impor.

Um dos pontos de grande discrepância de interpretações do texto da futura lei foi a relação entre o consentimento do titular e a transferência internacional. As conclusões acerca do papel do consentimento nas transferências foram diversas e, portanto, também as sugestões de mudança variaram.

Houve, por exemplo, o caso da *Brasscom* que negou a necessidade de consentimento para a transferência internacional para países com nível de proteção equiparável ao da lei e, paralelamente, a *Febraban* que sugeriu que as transferências para países com nível de proteção insatisfatório, mas dentro das exceções previstas à regra do artigo 28, não deveriam necessitar de consentimento especial.

Propostas avulsas para a regulação deste tema:

(A) A lei deve permitir transferências internacionais de dados pessoais independentemente do consentimento do titular para países que proporcionem nível de proteção comparável ao brasileiro.

Autor da proposta: *Brasscom.*

(B) A lei deve deixar mais claras as hipóteses de dispensa de autorização específica do órgão competente para transferências internacionais de dados pessoais.

Autor da proposta: *Febraban.*

Ainda sobre o consentimento para transferências internacionais, ocorreu um debate sobre a possibilidade de transferência internacional através de mero consentimento especial do titular de dados, como se verá abaixo.

Mais uma vez aqui podemos observar que há diferentes interpretações do texto do anteprojeto. Pode-se depreender, pelo teor das propostas, que o *GPoPAI* partiu do pressuposto de que este tipo de transferência seria permitido pela atual redação do anteprojeto, mas que os outros participantes entenderam que a redação original do anteprojeto vedava este tipo de prática.

4.25.1 Transferências internacionais de dados pessoais devem depender somente da autorização do titular?

Respostas controversas coletadas na plataforma de debate:

(A) Não.

Para o *GPoPAI,* a lei não deve admitir a possibilidade de transferência internacional de dados através de mero consentimento, mas sim incluir a necessidade de certificação internacional de *privacy by design* como hipóteses para autorização.

Quem defendeu isso? *GPoPAI*.

(B) Sim.

Para os defensores deste ponto, o consentimento do titular deve bastar para autorizar transferências internacionais. A regulação deste ponto deve estar de acordo com aquilo que é aplicado no resto do mundo, evitando, para isso, um regime que possa implicar em mais dificuldades e burocracias. Este artigo, em sua redação original, representaria um desestímulo à

variedade da oferta de produtos e serviços para os consumidores, assim como impossibilitaria trocas comerciais entre as empresas em diferentes países.

Quem defendeu isso? *Claro, Vivo, CNI, Brasscom* e *US Business Council.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais somente é permitida, nos seguintes casos:

I – Quando o titular dos dados consentir com a transferência de dados."

4.25.2. Propostas para desburocratização ou maior dinamismo no controle das transferências internacionais de dados pessoais

Para além da polêmica sobre o tratamento do consentimento nos casos de transferência internacional, muitos participantes opinaram que o regramento proposto na minuta do anteprojeto de lei apresentaria muitos obstáculos burocráticos ao fluxo de dados que ocorre na Internet. Tendo em vista este dito excesso de burocracia, foram propostas soluções para conferir à futura lei maior dinamismo ou menor rigidez neste controle. Neste sentido, *Fiesp* e *CNseg* opinaram que a referida legislação brasileira não tivesse a europeia como referência principal, inclusive com o intuito de se manter atualizada em relação às últimas tendências da inovação tecnológica.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve tornar a análise da legislação de outros países um elemento central da proteção de dados pessoais no Brasil.

O modelo adotado pelo APL teria se mostrado burocrático e ineficaz na Europa. O APL deve buscar o foco na responsabilização dos operadores e responsáveis pelo tratamento dos dados e retirar o foco da análise da legislação dos países em que estes agentes se encontram.

Autores da proposta: *ABEMD, Cisco, ITI, Névoa, GEPI-FGV, Giovanna Carloni* e *ABRANET.*

(B) A lei deve prever a possibilidade de adoção de acordos bilaterais com países sem nível adequado de proteção de dados.

"Com relação aos países sem nível adequado de proteção, sugerimos que se inclua no anteprojeto a

provisão de que se buscará adotar acordos semelhantes ao EUA - UE Safe Habour de forma a não estagnar as transações de dados".

Autores da proposta: *ABA* e *ABEMD.*

(C) A lei deve estabelecer que a proibição *ex ante* da transferência internacional de dados pessoais só poderá acontecer após determinação pelo governo brasileiro de que o país em questão não proporciona nível de proteção equiparado ao nacional.

"Para tais países a transferência internacional de dados deverá obedecer às condições que propomos estejam relacionadas em um parágrafo único deste artigo".

Autor da proposta: *SindiTeleBrasil.*

(D) A lei deve incluir a hipótese de autorização de transferência internacional de dados pessoais por obtenção de certificação internacional e/ou a atribuição, por parte das autoridades competentes de outros países, de atestado de que o ente realiza um tratamento adequado.

Autores da proposta: *GPoPAI, ABDTIC* e *Centre for Information Policy Leadership.*

(E) A lei deve utilizar o termo "adequado" em vez de "equiparável ao desta lei" para qualificar o nível de proteção que permite transferências internacionais de dados pessoais.

"Sugerimos a substituição do termo "equiparável ao desta lei" pelo termo "adequado". A exigência de um nível "equiparável" de proteção é ainda mais dura do que a abordagem da União Europeia sobre o tema e pode implicar em várias dificuldades para modelos de negócios online que envolvem o tratamento de dados sem fronteiras, uma vez que a redação adotada é muito restrita".

Autores da proposta: *MPA.*

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais é permitida, salvo quando houver manifestação expressa de órgão pertencente ao sistema jurídico brasileiro, que determinado país não proporciona nível de proteção de dados pessoais equiparável ao desta Lei.

4.25.3. Novas exceções para transferência internacional de dados pessoais para países com nível de proteção não equiparado ao estabelecido pela lei

Além disso, os participantes também sugeriram novas exceções para a regra geral do artigo 28, que determina a vedação de transferência para países com proteção não equiparável ao do anteprojeto.

Propostas avulsas para a regulação deste tema:

(A) A lei deve compatibilizar as exceções ao consentimento para tratamento de dados pessoais com as exceções para transferência internacional para países com nível de proteção não equiparado ao nela disposto.

Autor da proposta: *Centre for Information Leadership.*

(B) A lei deve incluir (i) cláusulas padrão entre processadores de dados e (ii) flexibilidade para transferências dentre um grupo empresarial ou um grupo de empresas que desenvolva uma atividade econômica em conjunto como exceções para transferência internacional de dados pessoais para países com nível de proteção não equiparado ao dela.

Autor da proposta: *BSA.*

(C) A lei deve incluir uma série de novas exceções à proibição da transferência internacional de dados para países que não proporcionem nível de proteção de dados equiparado ao da lei:

C1. Transferências necessárias para cumprir com obrigações legais e, de outro modo, cumprir com acordos contratuais;

C2. Transferências de interesse público ou interesse legítimo, tal como para prevenção de fraudes;

C3. Transferências necessárias no contexto de trabalho, atividade de recursos humanos e processos internos na empresa; e, por fim,

C4. Quando o titular forneceu anteriormente seu consentimento para a entidade responsável, permitindo que esta realizasse a transferência para um país que não possa fornecer o mesmo nível de proteção pessoal que o Brasil.

Autores da proposta: *US Business Council* (todas), *MPA* (**C1**, **C2** e **C3**), *CNseg* (**C1**) e *Febraban* (**C2** e **C3**)

Sugestões de redação:

Autor da sugestão: *Febraban.*

[INCLUSÃO] VI – quando a transferência ocorrer entre empresas do mesmo grupo econômico ou conglomerado multinacional, ou, ainda, ao operador que se obrigue formalmente aos termos desta lei;

Autor da sugestão: *US Business Council.*

[INCLUSÃO] VI – quando a transferência é necessária para cumprir com obrigações legais e de

outro modo cumprir com acordos contratuais;

VII – quando a transferência é de interesse público ou interesse legítimo, tal como prevenção contra fraudes, proteção à segurança de computadores e atividade de avaliação de riscos;

VIII – quando a transferência é necessária no contexto de trabalho, atividade de recursos humanos e processos internos na empresa;

IX – quando o titular forneceu anteriormente seu consentimento para a entidade responsável permitindo que esta realizasse a transferência para um país que não pode fornecer o mesmo nível de proteção pessoal que o Brasil;

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais é permitida, salvo quando houver manifestação expressa de órgão pertencente ao sistema jurídico brasileiro, que determinado país não proporciona nível de proteção de dados pessoais equiparável ao desta Lei.

Autor da sugestão: *Centre for Information Policy Leadership.*

[INCLUSÃO] VI – Quando a transferência ocorrer em uma das condições para a qual não é necessária autorização nos termos do Artigo 11.;

Autor da sugestão: *CNseg.*

[INCLUSÃO] VI – quando a transferência for necessária à execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular;

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais é permitida, no entanto, o órgão competente poderá excepcionar a transferência internacional de dados:

I – para assegurar a soberania e segurança nacional;

II – ou quando a transferência for necessária para a proteção da vida ou da incolumidade física ou psicológica do titular ou de terceiro;

III – ou quando o ordenamento jurídico do país de destino for manifestamente contrário aos princípios desta lei;

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível adequado de proteção de dados pessoais, ressalvadas as seguintes exceções:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 28. A transferência internacional de dados pessoais somente é permitida, nos seguintes casos:

I – Quando o titular dos dados consentir com a transferência de dados;

Autor da sugestão: *MPA.*

[INCLUSÃO] VI – quando as transferências não forem massivas e forem motivadas por interesses legítimos;

VII – quando os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional, podendo submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular;

VIII – para assegurar a constatação, o exercício ou a defesa de um direito perante o Poder Judiciário.

4.25.4. Transferências internacionais de dados pessoais necessárias para cooperação judicial entre órgãos de inteligência e de investigação

Neste inciso, os participantes *Giovanna Carloni* e *Lucas Silva Carrijo* destacaram que, não obstante a importância de estimular a cooperação internacional, o artigo deveria prever os instrumentos de direito internacional aos quais faz menção. A necessária previsão legal se faria necessária diante da possibilidade de este inciso legitimar a vigilância de governos estrangeiros por meio de dados pessoais coletados no Brasil.

4.25.5. Transferências internacionais de dados pessoais necessárias para a proteção da vida ou da incolumidade física do titular ou de um terceiro

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, ou ainda do responsável ou dos seus membros;

4.25.6. Autorização do órgão competente para a transferência internacional de dados pessoais para países com nível de proteção não equiparado ao estabelecido na lei brasileira

Propostas avulsas para a regulação deste tema:

(A) A lei deve exigir apenas consentimento do titular para a transferência internacional de dados para países com nível de proteção não equiparado ao da legislação brasileira, dispensando qualquer autorização adicional do órgão competente.

"*Desde que presente tal autorização, não faria sentido acrescentar outra etapa burocrática além da autorização dos titulares dos dados. O consentimento conforme o artigo 29 já é suficiente para alertar o titular de todos os riscos*".

Autor da proposta: *ABEP.*

(B) A lei não deve conferir um poder genérico ao órgão competente para autorizar transferências internacionais de dados pessoais.

"Este inciso consiste em delegação de poder vaga e genérica para um órgão cuja natureza jurídica sequer é prevista no anteprojeto. Desta forma, sugerimos a alterá-la para o texto previsto no caput do artigo 30, de forma que a exceção fique mais clara". (*MPA*)

"O inciso dá poderes para que a autoridade competente determine quais transferências podem ser autorizadas independentemente dos país destino dos dados. Diante da nebulosidade que cerca a autoridade competente, o inciso traz grande insegurança". (*ABDTIC*)

"O exame das jurisdições dos países destino dos dados consistirá em uma grande ônus administrativo. As leis de uma jurisdição não tem relação com a garantia do tratamento apropriado dos dados dentro de uma organização". (*ITI*)

Autores da proposta: *MPA, ABDTIC* e *ITI*.

4.26.7. Transferência internacional de dados pessoais resultante de compromisso assumido em acordo de cooperação internacional

Propostas avulsas para a regulação deste tema:

(A) A lei não deve autorizar genericamente transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao dela por força de compromissos assumidos em acordos de cooperação internacional.

"Esta lei deveria oferecer uma proteção mais efetiva contra a transferência de dados pessoais para países com nível de proteção menor do que o desta lei. A presente exceção oferece perigos ao respeito pela privacidade individual".

Autor da proposta: *Privacy International* e *Prof. Marcos.*

4.26.8. Transferências internacionais de dados pessoais necessárias para execução de política pública ou atribuição legal do serviço público

Propostas avulsas para a regulação deste tema:

(A) A lei não deve autorizar genericamente transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao dela em casos de necessidade para execução de política pública ou atribuição legal do serviço público.

"Este inciso deixa muito vulnerável o titular dos dados, posto que o governo poderá definir arbitrariamente e unilateralmente a transferência de dados pessoais, sem revisão dos demais poderes".

Autor da proposta: *ABDTIC.*

4.26.9. Avaliação do nível de proteção de dados pessoais de outros países pelo órgão competente

Propostas avulsas para a regulação deste tema:

(A) A lei deve incluir, na avaliação do nível de proteção de dados de outros países, a análise sobre a efetividade da regulação adotada e a existência de autoridades supervisoras independentes[28].

Autor da proposta: *Privacy International.*

(B) A lei deve fazer menção à edição, por parte do Poder Executivo, de regulamentação sobre os critérios específicos adotados para avaliação do nível de equivalência de proteção esperado.

Autor da proposta: *GEPI-FGV.*

(C) A lei deve aproximar os critérios para a avaliação do nível equivalência de proteção esperado aos adotados pela União Europeia.

Autor da proposta: *MPA.*

(D) A lei deve especificar as medidas de segurança que podem ser exigidas pelos regulamentos para que a transferência internacional de dados pessoais seja autorizada

[28] A contribuição foi realizada utilizando a seguinte terminologia, na língua inglesa: "*(a) rule of law, including national legislation in force and regulatory/professional rules; (b) existence and effective functioning of independent supervisory authorities to ensure compliance with the law*".

pelo órgão competente.

"*Inciso deve ser melhor esclarecido, vez que sugere que as medidas de segurança serão avaliadas diante dos regulamentos brasileiros. Entidades ao redor do mundo estabelecem suas medidas de segurança conforme o escopo de suas atividades, a obrigação de adotar medidas criadas em um determinado país provavelmente introduziria novos riscos, uma vez que as entidades não teriam capacidade para responder da forma dinamicamente necessária a uma mudança dos riscos*." (*ITI*)

"A sujeição da autorização da transferência internacional ao atendimento de medidas de segurança previstas em regulamento a ser expedido por órgão competente, resulta em grande ingerência do órgão público na estrutura de empresas.

As questões de segurança devem ser previstas em lei, a delegação da regulação de questões sensíveis para o executivo é grande ameaça aos direitos fundamentais. Além disso, estrutura para a segurança de dados em empresas são normalmente sigilosas". (*ABDTIC*)

Autores da proposta: *ITI* e *ABDTIC.*

Sugestões de redação:

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] II – natureza dos dados, origem e destinação;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~28~~ 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I – para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta ~~Lei, ressalvadas as seguintes exceções: I~~ Lei;

II – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional; ~~II~~

III – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; ~~III~~

IV – quando o órgão competente autorizar a ~~transferência, nos termos de regulamento; IV~~ transferência**;**

V – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; ~~V~~

VI – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do ~~§1º do~~ art. ~~6º~~ 24**.**

VII – quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

Parágrafo único. O nível de proteção de dados do país será avaliado ~~por~~ pelo órgão competente, que levará em conta:

I – normas gerais e setoriais da legislação em vigor no país de destino;

II – natureza dos dados;

III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV – adoção de medidas de segurança previstas em regulamento; e

V – outras circunstâncias específicas relativas à transferência.

4.27. Consentimento especial para transferência internacional de dados a países com nível de proteção não equiparado ao da lei

REDAÇÃO LEVADA A DEBATE

Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:

I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e

II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.

Este artigo dispõe sobre a necessidade de consentimento especial para autorização de transferências internacionais para países sem o nível adequado de proteção de dados pessoais.

Propostas avulsas para a regulação deste tema:

(A) A obtenção de consentimento especial não deve ser a única alternativa para autorização de transferência internacional de dados pessoais para país com nível de proteção não equiparado ao da lei.

"Esse Artigo (29) não prevê os importantes mecanismos de transferências de dados, como, por exemplo, códigos de conduta, ou disposições contratuais flexíveis que garantem que os dados sejam tratados de forma apropriada. Esses mecanismos internacionalmente reconhecidos devem ser autorizados, como uma alternativa ao consentimento.

Ainda, não está claro se a referência no Artigo 7 sugere que seria necessário um consentimento distinto para a transferência (em acréscimo ao consentimento para a coleta inicial). Esses dois níveis de consentimento seriam inviáveis". (ITI)

Autores da proposta: *ITI e Câmara BR.*

(B) A lei deve criar uma exceção à regra de obtenção de consentimento especial no caso de transferência interna dentro de uma mesma empresa.

Autores da proposta: *ABRANET e Câmara BR.*

(C) A lei deve estabelecer que transferências internacionais sem o consentimento do titular dos dados pessoais exijam autorização pela Justiça Federal.

Auto da proposta: *Rodrigo Veleda.*

(D) A lei não deve estabelecer a necessidade de obtenção de consentimento especial para casos de transferências internacionais de dados pessoas a países com nível de proteção não equiparado ao dela.

"Sugerimos a eliminação deste artigo. Isso porque o consentimento é condição necessária e suficiente para a autorização de transferências internacionais. Não sendo, portanto, necessários outros mecanismos adicionais.

Ademais, a própria estrutura da lei, que estabelece responsabilidade solidária para responsáveis pela tratamento e operadores (artigo 31), já protege o usuário" (ABDTIC).

Autores da proposta: *Brasscom, Vivo, SindiTeleBrasil e ABDTIC.*

(E) O consentimento especial para o caso de transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao da lei não é suficiente para proteger o titular.

"*A transferência internacional de dados para países com menor nível de proteção nunca deveria ser permitida. As previsões dos incs. I e II, para que o titular seja previamente informado quanto aos*

riscos, a fim de manifestar seu consentimento, não é suficiente. Trata-se de situação com alto grau de complexidade a respeito da qual o titular tem condições muito reduzidas de formar um juízo a respeito" (*Proteste*).

"*Ademais, a exceção à regra do artigo 28 caso haja consentimento - ainda que especial - parece fragilizar a proteção do titular ao colocar sobre o indivíduo uma responsabilidade excessiva com relação à gestão de seus dados*" (*CTS-FGV*).

"A privacidade deve ser um valor na fase de desenvolvimento de softwares e hardwares, de modo que as próprias aplicações tenham nelas imbuído tal valor (e esse o conceito de privacy by design). Propõe-se a operacionalização desse conceito mediante vinculação do operador às cláusulas contratuais-padrão. Desta forma, sugerimos alteração no art. 29". (*GPoPAI*)

Autores da proposta: *CTS-FGV, GEPI-FGV, GPoPAI e Proteste.*

(F) Para maior eficácia e responsabilização dos agentes envolvidos, devem ser criadas obrigações adicionais sobre a forma de obtenção de consentimento especial para casos de transferências internacionais de dados pessoas a países com nível de proteção não equiparado ao da lei.

"Diante da dificuldade de se verem vistas cumpridas as disposições deste artigo principalmente por causa do grande número de sites estrangeiros acessados em território nacional, sugere-se a inclusão de dois parágrafos no artigo que visam: (1º) dar maior conhecimento ao usuário e (2º) deixar claro que o consentimento não exime as empresas de responsabilidade".

Autora da proposta: *Veridiana/Intervozes.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~29~~. ~~Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:~~

~~**I** – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e~~

~~**II** – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.~~

4.28. Autorização para transferências internacionais de dados pessoais para países com nível de proteção não equiparado ao da lei

REDAÇÃO LEVADA A DEBATE

Art. 30. A autorização referida no inciso III do caput do art. 28 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

Propostas avulsas para a regulação deste tema:

(A) Não devem ser criadas obrigações adicionais relacionadas à autorização para transferências internacionais de dados pessoais para países com nível de proteção não equiparado ao da lei.

"O artigo em questão deve ser excluído. Observamos que a exigência de cláusulas contratuais específicas, previamente aprovadas, cria um grande ônus de natureza administrativa ao órgão

competente" (ITI).

"Sugerimos a eliminação do artigo. Isso porque o mecanismo das cláusulas contratuais gerais para a transferência internacional de dados pode vir a ser limitador para a realização de transações, transações estas que são vitais para concluir determinadas operações comerciais dos titulares dos dados, na medida em que o fluxo de dados e as atividades econômicas que dele dependem são inerentemente globais.

Defendemos que as transferências internacionais sejam realizadas através da obtenção de consentimento dos titulares ou, alternativamente, através de mecanismos de transferência internacional de dados que garantam a segurança do tráfego mediante a garantia do cumprimento de determinados parâmetros de privacidade, como, por exemplo, o sistema APEC Cross-Border Privacy Rules". (*Vivo*)

Autores da proposta: *ABDTIC, SindiTeleBrasil, Fiesp, ITI* e *Vivo.*

(B) A adoção de cláusulas-padrão ou modelos internacionais reconhecidos pelo Brasil deve substituir qualquer outra exigência e ser suficiente para que transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao da lei sejam válidas.

Autores da proposta: *ABRANET e Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 30. O órgão competente poderá autorizar a transferência internacional de dados pessoais somente na hipótese do art. 28, inciso III, quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

4.28.1. A lei deve possibilitar que o órgão competente crie cláusulas contratuais-padrão obrigatórias para autorizar transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao brasileiro?

Respostas controversas coletadas na plataforma de debate:

(A) Não, a lei não deve obrigar a adoção de cláusulas contratuais-padrão, pois isso contrariaria o princípio da autonomia da vontade.

"A autonomia da vontade, disposta no CC em seu artigo 421, garante aos particulares possibilidade de elaborar e firmar negócios independentemente da intervenção estatal na ordem econômica, a qual, conforme é sabido, pode resultar em entraves ou irregularidades no processo de desenvolvimento econômico a longo prazo. Nem mesmo na seara do código de defesa do consumidor

há o estabelecimento de contratos padrão pelo órgão regulador.

Ao contrário, o que é possível, e mesmo recomendável, que ocorra é a fixação de bases principiológicas direcionando o conteúdo dos instrumentos postos à disposição dos consumidores, bem como o controle posterior sobre eventual contradição".

Quem defendeu isso? *Febraban e ITI.*

(B) Sim.

"É acertada a escolha do APL por incorporar cláusulas contratuais padrão e regras societárias globais, posto que são conceitos fundamentais para alinhar o Brasil com os padrões europeus de transferências de dados internacionais. Porém, esses mecanismos têm suas respectivas limitações, as cláusulas contratuais podem resultar em uma desnecessária complexidade e as regras societárias globais se limitam a transferências dentro de um grupo de empresas e sem perspectivas de maior abrangência. Diante desses limites, recomendamos que as autoridades trabalhem com especialistas experientes nesses tipos de mecanismo com o objetivo de torná-los mais práticos e amplamente utilizáveis".

Quem defendeu isso? *Centre for Information Policy Leadership.*

4.28.2. Responsabilização solidária e autorização para transferências internacionais de dados pessoais a países com nível de proteção não equiparado ao da lei

Propostas avulsas para a regulação deste tema:

(A) A lei não deve responsabilizar o cedente que realize auditoria sobre organização do cessionário.

Autor da proposta: *ITI.*

(B) A lei deve permitir que cedente e cessionário disponham da responsabilidade em contrato.

"Sugere-se a exclusão da responsabilidade solidária e consequente permissão da alocação de responsabilidade por acordo entre as partes.

Embora as cláusulas contratuais padrão possam ser úteis, é importante que não sejam consideradas o único método para criar mecanismos para transferência de dados. Além disso, tais cláusulas padrão devem permitir que as partes em contratos comerciais cheguem a um acordo quanto à responsabilidade, desde que as responsabilidades sejam totalmente detalhados, uma vez que em muitos acordos de transferência exigir a responsabilidade solidária é inadequado, especialmente quando uma das partes é muito maior".

Autor da proposta: *US Business Council.*

(C) A lei deve estabelecer que a responsabilidade será atribuída de acordo com a participação no evento danoso.

Autores da proposta: *Febraban, ABRANET e Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Centre For Information Policy Leadership.*

[MODIFICAÇÃO] § 1º O Órgão competente poderá elaborar cláusulas contratuais-padrão para transferências de responsável pelo tratamento para responsável pelo tratamento e de responsável pelo tratamento para operador, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independentemente de culpa, de cedente e cessionário. O uso de cláusulas contratuais padrão não estará sujeito à autorização individual mencionada na Seção II do caput do Artigo 28.

4.28.3. Normas corporativas globais como meio de obtenção de permissão para transferências internacionais de dados pessoais dentro do mesmo grupo econômico

Propostas avulsas para a regulação deste tema:

(A) A lei deve reconhecer mecanismos já existentes de aprovação de normas corporativas globais, como o *Binding Corporate Rules* estabelecido na União Europeia.

Autores da proposta: *Câmara BR, ABINEE e ABRANET.*

(B) A lei deve estabelecer isonomia entre "responsáveis" e "operadores" quando dispões sobre a capacidade de desenvolver normas corporativas globais e submetê-las como meio de obter permissão para transferências internacionais de dados pessoais.

Autor da proposta: *ITI.*

(C) A lei deve permitir transferências internacionais de dados pessoais feitas no âmbito de um mesmo grupo econômico ou de parcerias entre responsáveis pelo tratamento.

"Sugerimos nova redação para o dispositivo. Dados devem ser livremente transferidos dentro de um mesmo grupo econômico ou no âmbito de parcerias entre responsáveis pelo tratamento. Ressalta-se que estes dados devem ter sido colhidos mediante o consentimento dos titulares".

Autor da proposta: *Vivo.*

(D) A lei deve permitir o uso de outros mecanismos para certificação de transferências internacionais de dados pessoais, como selos de privacidade interoperáveis.

"Incentivamos também o uso de outros mecanismos de transferências internacionais que facilitem transferências que não são feitas entre empresas, como marcas e selos de privacidade e outros códigos de conduta organizacional que são certificados por terceiros apropriados ou por um órgão

competente.

Ainda sobre as marcas e selos de privacidade, é recomendável que os mecanismos adotados no Brasil sejam 'interoperáveis' com outros mecanismos de transferência internacional semelhantes, dessa forma, empresas não precisaram ser aprovadas por mais de um regime, bastando que sejam aprovadas por um regime com requisitos semelhantes ao brasileiro".

Autor da proposta: *Centre for Information Leadership.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] § 2º A transferência internacional de dados pessoais é permitida entre os responsáveis pelo tratamento que façam parte de um mesmo grupo econômico, conglomerado multinacional ou parceiros, sem necessidade de autorizações específicas, observado o cumprimento das normas relativas à obtenção do consentimento por parte do titular dos dados no País do(s) responsável(is) pelo tratamento dos dados.

Autor da sugestão: *Centre for Information Leadership.*

[MODIFICAÇÃO] § 2 Os operadores e responsáveis, ou grupos de operadores e responsáveis, podem enviar regras empresariais globais aplicáveis para aprovação pelo órgão competente ou regras empresariais globais que tenham sido aprovadas por um órgão competente estrangeiro, ou podem apresentar comprovação de participação em um código de conduta transfronteiriça aplicável ou um selo ou marca de privacidade, sem necessidade de autorizações específicas até o limite em que esses instrumentos cumpram, os princípios gerais de proteção e os direitos do titular de dados.

4.28.4. Poder de requisição de informações suplementares e diligências na análise de cláusulas contratuais ou normas corporativas globais por parte do órgão competente

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar um modelo de aprovação automática de cláusulas contratuais pelo órgão competente.

Os participantes que sugeriram esta proposta entendem que a aprovação das cláusulas seria um processo trabalhoso e burocrático demais, que criaria acúmulos de pedidos, provocando a "inundação" do órgão por solicitações. A busca de informações adicionais seria em caso de alterações nas cláusulas padrão adotadas pelo cedente e cessionário.

Autores da proposta: *US Business Council, ITI.*

Sugestões de redação:

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] § 3º Caso sejam feitas alterações à cláusula contratual padrão ou normas corporativas mundiais, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

4.28.5. Novas propostas sobre autorização para transferência internacional de dados

Propostas avulsas para a regulação deste tema:

(A) A lei precisa definir que o órgão competente considere a possível natureza global do processamento de dados, não vinculando suas autorizações e aprovações ao cumprimento de garantias que ensejem conflito com leis vigentes em outras jurisdições.

"Ao lado de normas corporativas globais limitadas ao mesmo grupo econômico ou conglomerado internacional, tal como disposto no §2º do art. 30, também pode ser considerada a adesão a normas como o European BCR (Binding Corporate Rules ou Normas Corporativas de Cumprimento Obrigatório) como forma de demonstrar a aderência dessas empresas a padrões globais de proteção de dados, sendo desnecessária a aprovação do órgão competente para que procedam à transferência internacional de dados dentro do grupo ou conglomerado".

Autores da proposta: *Brasscom.*

(B) O órgão competente deve ser obrigado por lei a divulgar, periodicamente, listas contendo países que apresentam níveis adequados de proteção de dados.

"[Para] *evitar* [que] *a necessidade que empresas procurem a autoridade a procura desse tipo de informação".*

Autores da proposta: *CNseg.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 4º O órgão competente deve levar em consideração a possível natureza global da operação de processamento, não devendo vincular suas autorizações e aprovações ao cumprimento de garantias que possam ensejar o conflito com leis atualmente em vigor em outras jurisdições a que os mesmos grupos econômicos operando no Brasil também estejam submetidos.

Autor da sugestão: *CNseg.*

[MODIFICAÇÃO] § 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.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 30**~~ **34**. A autorização referida no inciso ~~III~~ IV do caput do art. ~~28~~ 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º ~~Órgão~~ O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária~~, independente de culpa, de~~ do cedente e do cessionário, independentemente de culpa.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação ~~de~~ do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais, documentos ou de normas corporativas globais submetidas à aprovação ~~de~~ do órgão competente,

poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §1° e §2° do artigo 45.

4.29. Responsabilidade solidária do cedente e cessionário pelo tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.

4.29.1. A responsabilidade deverá ser solidária nos casos de tratamento de dados no exterior e no território nacional?

Respostas controversas coletadas na plataforma de debate:
(A) Sim. "*Esse dispositivo, que responsabiliza solidariamente o cedente e o cessionário pelo tratamento de dados no exterior ou no território nacional, é suficiente para inibir qualquer comportamento inapropriado à luz dos princípios e objetivos desejados pelo APL*". **Quem defendeu isso?** *SEAE/MF.*
(B) Não, a cada um dos agentes deve ser atribuída responsabilidade apenas por seus próprios atos. Os defensores dessa posição sugerem a supressão do artigo e argumentam que o conceito de responsabilidade solidária nos casos de transferência internacional poderia acarretar uma responsabilidade indevida dos agentes envolvidos em uma operação de tratamento e, consequentemente, em insegurança jurídica. **Quem defendeu isso?** *Câmara BR, MPA, BRASSCOM, Febraban, ABINEE, US Business Council* e *ABRANET.*
(C) Não, mas o cedente deverá estar obrigado a conduzir uma auditoria apropriada e

adotar medidas razoáveis para garantir o tratamento apropriado de dados pelo cessionário.

"*A responsabilidade solidária criará um desincentivo financeiro para a terceirização, análise e criação de nuvens no mercado brasileiro, uma vez que tanto o responsável quanto o operador precisarão considerar o possível impacto financeiro e operacional sobre os atos indevidos praticados pela outra parte*".

Quem defendeu isso? *ITI.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] O cedente e o cessionário são responsáveis, nos limites de sua atuação, pelos danos ocasionados no tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, observado o disposto no §2º do artigo 35.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~31~~ 35. O cedente e o cessionário ~~têm responsabilidade~~ respondem solidária e objetivamente pelo tratamento de dados ~~realizado no exterior ou no território nacional~~, independentemente do local onde estes se localizem, em qualquer hipótese~~, independente de culpa.~~

4.30. Permissão de tratamento de dados pessoais transferidos de país estrangeiro

REDAÇÃO LEVADA A DEBATE

Art. 32. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve criar obrigação de observância a normas relativas à obtenção do consentimento para permitir o tratamento de dados pessoais transferidos de país estrangeiro no território nacional.

Os defensores dessa posição advogam pela exclusão do artigo, pois ele traria uma responsabilidade adicional para agentes brasileiros, que passariam a ter de analisar o cumprimento de legislação exógena. Ele acabaria por se tornar em um "agente de polícia" por ter que garantir a fiscalização, bem como o cumprimento da legislação estrangeira.

Autores da proposta: *GSMA, Brasscom, Vivo, SindiTeleBrasil, Centre For Information Policy Leadership, ABDTIC, CNseg, SEAE/MF e ITI.*

(B) A lei deve permitir o tratamento de dados pessoais transferidos de países estrangeiros no território nacional apenas quando o nível de proteção deste país for equiparado ao brasileiro.

"A determinação de que o cessionário baseado no Brasil tenha que verificar os termos pelos quais foi realizado tratamento no estrangeiro deve ser evitada. Isso porque não é razoável exigir o conhecimento da legislação de cada país que transmita dados para o Brasil.

O recomendado é seguir a redação do artigo 28 deste Anteprojeto, que dispõe que as transferências internacionais devem ocorrer entre países que proporcionem nível de proteção equiparável a este Anteprojeto, já que a simples observâncias às normas do país cedente pode não ter o mesmo efeito protetivo ora objetivado".

Autores da proposta: *Febraban.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 32. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observados os princípios desta lei.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 32.** No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.~~

4.31. Normas suplementares para identificação de operação de tratamento como transferência internacional de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

Propostas avulsas para a regulação deste tema:

(A) O órgão competente não deve ter poderes de editar normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

Alguns defensores dessa proposta argumentam que o poder dado à autoridade competente seria discricionário e conferiria a ela liberdade para criar normas limitadoras ou excessivas, sem a devida discussão necessária.

A *ABEP*, por sua vez, sugere a exclusão do artigo "*posto que o conceito transferência internacional é natural e suficientemente claro, dispensando explicitação*".

Autores da proposta: *Câmara BR, ABRANET, Brasscom, MPA, SindiTeleBrasil* e *ABEP.*

(B) As normas complementares editadas pelo órgão competente não serão capazes de acompanhar as inovações em matéria de transferência de dados e tornar-se-ão uma barreira burocrática a processos inovadores e à concorrência.

Este dispositivo é inadequado para um mundo globalizado, em que se mudam de maneira constante os fluxos de dados e a forma como esses dados são coletados, distribuídos e tratados. Além disso, as "*Data-driven innovations*" tenderão a mudar mais rapidamente do que qualquer norma regulamentar pode se adaptar, o que faz a regulamentação ser apenas uma barreira que aumenta a carga burocrática sobre processos inovadores e dificulta a concorrência. Sugere a supressão desse artigo.

Autores da proposta: *SEAE/MF.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 33.** Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.~~

4.32. Responsabilidade civil dos agentes do tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

CAPÍTULO VII – RESPONSABILIDADE DOS AGENTES

Seção I – Agentes do Tratamento e Ressarcimento de Danos

Art. 34. São agentes do tratamento de dados pessoais o responsável e o operador.

Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.

§ 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;

§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.

4.32.1. Qual deve ser a responsabilidade civil dos agentes de tratamento de dados pessoais?

A discussão em torno dessa pergunta é muito importante para a aplicação da futura lei de proteção de dados no Judiciário. As opiniões dos participantes se dividiram de forma clara em três vertentes.

A primeira vertente representa aqueles que acreditam que a responsabilidade deve ser subjetiva. Assim, defendem que, na ocasião de uma eventual ofensa a direitos, deve ser verificada a existência de culpa ou dolo. A segunda agrupou os que argumentaram pela escolha da responsabilidade objetiva – independente de culpa – em razão de considerarem o tratamento de dados uma atividade de risco.

Por fim, a terceira vertente sugeriu que somente o responsável pelo tratamento deveria ser responsabilizado perante o titular e o órgão competente, já que ele seria quem detém todas as informações acerca dos titulares de dados e dos próprios dados que estariam sendo tratados.

Respostas controversas coletadas na plataforma de debate:

(A) A responsabilidade dos agentes de tratamento deve ser subjetiva.

Defensores dessa posição entendem que elementos subjetivos (culpa ou dolo) devem ser levados em conta para determinar a responsabilidade de agentes de tratamento de dados pessoais. Defendem também que devem ser estabelecidos critérios legais para verificação de dolo, bem como balizas de valor apropriado para ressarcimento.

Quem defendeu isso? *ITI* e *SindiTeleBrasil*.

(B) A responsabilidade dos agentes de tratamento deve ser objetiva.

Os participantes que defenderam essa posição argumentam que o tratamento de dados deve ser visto como uma atividade de risco, a qual inclusive requereria medidas de segurança. Esta sugestão estaria alinhada com a tendência nas demais relações de consumo segundo a qual quem exerce uma atividade de risco só é eximido de responsabilidade em caso de culpa exclusiva da vítima ou força maior.

Quem defendeu isso? *GPoPAI, Veridiana/Intervozes, Luiz Perin Filho* e *Joana Varon.*

(C) Somente o responsável deverá ser responsabilizado. Cabendo ao operador responder apenas por violação contratual.

Alguns participantes opinaram pela criação de regimes de responsabilidade jurídica diferentes entre responsáveis e operadores. Somente o responsável pelo tratamento deveria, em sua opinião, ser responsabilizado. Caberia ao operador, portanto, responder apenas em casos de violação de seu contrato com o responsável.

O argumento é de que somente o responsável pelo tratamento deteria informações sobre a relação com o consumidor, quais bases e sob quais condições os dados estariam sendo manipulados e quais dados seriam armazenados no sistema. Além disso, seria o próprio responsável pelo tratamento quem escolheria e imporia exigência relativas ao tratamento ao operador.

Quem defendeu isso? *Câmara BR, Fiesp, ABINEE, ABDTIC e ABRANET*.

Sugestões de redação:

Autor da sugestão: *GPoPAI.*

[MODIFICAÇÃO] Art. 35. O tratamento de dados pessoais é atividade de risco e todo aquele que, em razão do exercício de tal atividade, casar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, independentemente de culpa, nos termos desta lei

§1. A exclusão da responsabilidade do operador e dos demais agentes que integram a cadeia de tratamento de dados pessoais somente se dará nos casos de culpa exclusiva da vítima ou força maior.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 35. Todo aquele que, nos limites de suas atividades, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos do Código Civil e legislação correlata. A atuação fora dos limites das atribuições legais sujeitará a responsabilização nos termos da legislação em vigor.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, e que função dos descumprimentos desta Lei e da regulamentação aplicável, venha a causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.

4.32.2. Novas propostas sobre o regime de responsabilidade jurídica dos agentes do tratamento de dados pessoais.

Propostas avulsas para a regulação deste tema:

(A) A lei deve limitar a reparação de danos causados por agentes do tratamento de dados pessoais aos titulares aos casos dados materiais por estes comprovados, excluindo a possibilidade de indenizações por danos morais.

"Sugerimos limitar danos a situações onde os titulares dos dados possam demonstrar danos materiais. Permitir reivindicações com base em danos "morais" criará um grande número potencial de reivindicações impraticáveis, muitas delas baseadas em argumentação subjetiva. Isso poderia resultar em desviar o sistema judiciário brasileiro de casos verdadeiramente prioritários, atrasando a capacidade daqueles verdadeiramente prejudicados de seu direito a uma audiência".

Autores da proposta: *US Business Council.*

Sugestões de redação:

Autor da sugestão: *US Business Council.*

[MODIFICAÇÃO] § 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Parágrafo Único. O juiz, nos termos da legislação em vigor, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa.

4.32.3. Ônus da prova em responsabilização de agentes de tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei não deve inverter o ônus da prova em casos em que um titular de dados pessoais requeira a responsabilização de agentes de tratamento em razão de prejuízo financeiro resultante de descumprimento de obrigação legal.

Autor da proposta: *ITI.*

(B) A lei deve determinar que, diante da comprovação de dano causado ao titular de dados pessoais, os agentes do tratamento somente não devem ser responsabilizados caso indiquem e comprovem o causador do dano.

Autor da proposta: *Prof. Marcos.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

CAPÍTULO ~~VII~~ VI – ~~RESPONSABILIDADE DOS~~ AGENTES DO TRATAMENTO DE DADOS PESSOAIS

Seção I – ~~Agentes do Tratamento~~ Responsável e ~~Ressarcimento de Danos~~ Operador

Art. ~~34~~. 36. São agentes do tratamento de dados pessoais o responsável e o operador.

~~**Art. 35.** Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.~~

~~**§ 1º** O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;~~

~~**§ 2º** O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.~~

4.33. Eventual dispensa da exigência do consentimento e observância dos princípios gerais e garantias dos direitos do titular de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 36. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Este artigo não recebeu contribuições durante o debate público.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi suprimido conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 36.** A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei,~~

~~especialmente da observância dos princípios gerais e da garantia dos direitos do titular.~~

4.34. Aplicação de punições cabíveis a agentes do tratamento de dados pessoais de órgãos públicos

REDAÇÃO LEVADA A DEBATE

Art. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, conforme disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar um portal para publicação de infrações e acompanhamento dos casos.

Autor da proposta: *Thiago.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 37. ~~As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores~~ O responsável e ~~responsáveis~~ o operador devem manter registro das operações de ~~órgãos públicos que agirem~~ tratamento de ~~forma contrária a esta Lei, conforme disposto na Lei no 8~~ dados pessoais que realizarem~~.112, de 11 de dezembro de 1990 e na Lei no 8~~

Parágrafo único.~~429~~ **O** órgão competente poderá dispor sobre formato, estrutura e tempo de ~~2 de junho de 1992~~ guarda do registro.

4.35. Competências e responsabilidades relativas à gestão de base de dados de órgão públicos e a atos administrativos

REDAÇÃO LEVADA A DEBATE

Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer um regime de responsabilidade objetiva do Estado na gestão de bases de dados pessoais e prática de atos administrativas referentes a dados pessoais.

"O sistema de responsabilidade civil objetiva deve, também, ser adotado em face do Estado. O tratamento de dados pessoais deve ser considerado uma atividade de risco, isto, por si só, já demanda a aplicação da responsabilidade objetiva. Tal entendimento deve ser reforçado nos casos em que o responsável pelo tratamento é órgão ou entidade do poder público, inclusive por causa do disposto na CF no artigo 37, parágrafo 6º" (*Veridiana/Intervozes*).

"Entendemos que não há justificativa para que a responsabilização decorrente de ato ilícito praticado por qualquer dos agentes que atuem na cadeia de coleta e tratamento de dados seja subjetiva, dependendo da apuração de culpa, o que prolongará o curso de processo judicial, prejudicando injustamente o cidadão ou consumidor. Defendemos que a responsabilidade deve seguir o mesmo regime estabelecido pelo Código de Defesa do Consumidor" (*Proteste*).

Autores da proposta: *Luiz Perin Filho, Veridiana/Intervozes, GPoPAI, Proteste* e *Joana Varon.*

(B) A lei deve determinar que o órgão competente seja responsável pela interpretação das regras existentes, em respeito ao princípio da legalidade.

Autor da proposta: *Brasscom.*

(C) A lei deve estipular um prazo para que sejam editados atos normativos sobre competência e responsabilidade por gestão de bases de dados e atos administrativos referentes a dados pessoais.

Autor da proposta: *Jhonata Goulart Serafim.*

Sugestões de redação:

Autor da sugestão: *Jhonata Goulart Serafim.*

[INCLUSÃO] Parágrafo Único: Os atos normativos citados no caput deverão ser criados no prazo

de 120 dias contados da publicação da presente lei.

Autor da sugestão: *Proteste.*

[MODIFICAÇÃO] Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão objetivas, ressalvado o direito de regresso por dolo ou culpa, nos termos do art. 37, § 6º, da Constituição Federal.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências, observados os limites estabelecidos em Lei..

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi suprimido conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 38.** As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.~~

4.36. Responsável e operador: definições e responsabilidades.

REDAÇÃO LEVADA A DEBATE

Seção II – Responsável e Operador

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

§ 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.

> **§ 2º** Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

4.36.1. Atribuições legais do operador do tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer que o operador não tem direitos próprios sobre os dados, ficando sua atividade restrita à prestação de serviços por conta do responsável.

"Deve-se deixar claro no artigo que o operador não tem direitos próprios sobre os dados, devendo somente prestar serviços por conta do responsável. (Não pode reprocessar, vender, utilizar fora do escopo do contrato, etc.)".

Autor da proposta: *Daniel Astone.*

4.36.2. As figuras do "operador" e do "responsável" devem ser solidariamente responsáveis pelas operações de tratamento?

A discussão acerca da responsabilização solidária se coloca como um ponto muito importante na discussão do anteprojeto, permeado por divergência entre as opiniões dos participantes.

Na hipótese de uma escolha pela responsabilidade solidária, havendo danos aos direitos dos titulares de dados durante o tratamento realizado pelo operador, tanto ele como o responsável pelo tratamento poderiam ser totalmente responsabilizados. Nesse sentido, após resolvida a contenda com o titular, cada um poderia então se valer de um direito de regresso em relação ao outro ou de direitos estabelecidos contratualmente.

A solidariedade, portanto, facilitaria que o dano causado ao titular seja compensado já que tanto operador quanto responsável serão responsabilizados por todo o dano. No entanto, como se verá, foi apontado enquanto crítica que esse regime acabaria por prejudicar de forma indevida agentes envolvidos no tratamento de dados.

Respostas controversas coletadas na plataforma de debate:

(A) A responsabilidade deve ser solidária.

Os participantes defensores dessa posição apontaram para o fato de que, muitas vezes, o titular não tem ideia de que operador e o responsável são pessoas distintas e, por isso, um regime de

responsabilidade solidária seria necessário. Por meio dele, o direito de regresso seria prestigiado e haveria um estímulo para que o operador (e não só o responsável) atuasse em conformidade com as normas aplicáveis à matéria.

Quem defendeu isso? *ABEMD, ABDTIC* e *Proteste*.

(B) A responsabilidade não deve ser solidária.

Os participantes que defenderam essa posição sugerem a supressão do artigo. Para eles, somente o responsável pelo tratamento deveria ser responsabilizado perante a autoridade e ao consumidor, pois somente o responsável pelo tratamento conheceria a relação com o consumidor e as condições sob as quais os dados estão sendo manipulados e armazenados no sistema. Além disso, defendem que é o próprio responsável quem escolhe o operador, o nível de segurança necessário e determina exigências ao operador. Com relação ao operador só caberia responsabilidade em caso de quebra do seu contrato com o responsável.

Quem defendeu isso? *Câmara BR, Brasscom, MPA, Febraban, US Business Council, ABINEE e Cisco.*

(C) A responsabilidade deve ser solidária em regra, ressalvado o caso em que o operador atue sem contemplar as instruções dadas pelo responsável.

Quem defendeu isso? *SindiTeleBrasil*.

(D) A responsabilidade não deve ser solidária em regra, mas o responsável que não se assegure de que o operador está conduzindo o tratamento devidamente deve ser solidariamente responsabilizado.

Quem defendeu isso? *ITI.*

Sugestões de redação:

Autor da sugestão: *ABEMD.*

[MODIFICAÇÃO] § 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador, ressalvado àquele o direito de regresso.

Autor da sugestão: *Câmara BR .*

[MODIFICAÇÃO] § 1º O responsável tem responsabilidade quanto a todas as operações de tratamento realizadas pelo operador, salvo quando este agir em desacordo com as instruções do responsável.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador em conformidade com as instruções recebidas.

4.36.3. Determinação para o responsável elaborar relatório de impacto à privacidade

Propostas avulsas para a regulação deste tema:

(A) A lei não deve conceder ao órgão competente a competência de determinar que o responsável elabore relatório de impacto à privacidade de suas operações de tratamento.

"Exclusão do parágrafo. O parágrafo faculta ao órgão competente a criação de mecanismos de controle sem uma clara definição, em âmbito de Lei, de parâmetros e limites para a sua implementação. Tal redação poderia levar a má interpretação no sentido de permitir que o órgão competente viesse a criar novas obrigações que apenas o legislador poderia estabelecer, exacerbando o escopo regulador que deve nortear a atuação do órgão". (*Brasscom*)

Autores da proposta: *GSMA, Claro, Vivo e SindiTeleBrasil* e *Brasscom.*

(B) A lei deve determinar que os relatórios de impacto a privacidade que serão produzidos a pedido do órgão competente trarão estatísticas abrangidas nas operações de tratamento de dados, de modo a respeitar a proteção do segredo empresarial de informações.

Autor da proposta: *Febraban.*

(C) A lei deve estabelecer que a determinação de elaboração de relatórios de impacto a privacidade precisa ser fundamentada e trazer explicação sobre as circunstâncias que exigiram a avaliação, os elementos a serem avaliados e quem terá acesso ao documento.

Autor da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] § 2º Órgão competente poderá determinar, mediante decisão fundamentada e critérios objetivos, ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] § 2º Órgão competente poderá determinar ao responsável que elabore relatório

estatístico de impacto à privacidade referente às suas operações de tratamento de dados, ressalvados os dados que sejam relacionados a segredo empresarial, nos termos do regulamento.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Seção II – Responsável e Operador**~~

Art. ~~**39.**~~ **38.** O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

~~**§ 1º** O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.~~

Art. 39. ~~**§ 2º** Órgão~~ O órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

4.37. Dever de manutenção de registro das operações de tratamento de dados pessoais pelo responsável ou operador

REDAÇÃO LEVADA A DEBATE

Art. 40. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, observado o disposto no art. 15.

Parágrafo único. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve criar um dever de registro das operações de tratamento de dados pessoais pelo responsável ou pelo operador.

Os defensores dessa proposta advogam pela supressão do artigo por considerarem que ele inviabiliza a atividade empresarial de tratamento de dados pessoais na prática, além de não

constituir um dever de cumprimento claro (não há prazo para a guarda desses registros).

Autores da proposta: *Claro, SindiTeleBrasil, Associação da Liberdade Religiosa e Negócios.*

(B) A lei deve estabelecer um prazo para a guarda e um maior detalhamento dos registros obrigatórios das operações de tratamento de dados pessoais pelo responsável ou pelo operador.

Autor da proposta: *GSMA.*

(C) A lei deve estabelecer um porte econômico mínimo para incidência de um dever de registro das operações de tratamento de dados pessoais pelo responsável ou pelo operador.

"Dessa forma, será possível exigir o investimento adequado para melhor conservar as informações pessoais, sem que se fira a inovação e pequenos empreendedores do mercado brasileiro".

Autor da proposta: *Roberto Taufick.*

(D) A lei não deve criar um dever de registro das operações de tratamento de dados pessoais pelo operador, mas somente pelo responsável.

"Somente o Responsável pelo tratamento deve manter os registros. Isso porque somente ele tem conhecimento completo da cadeia e da base jurídica, desde o consumidor até o operador".

Autores da proposta: *ABINEE.*

(E) O dever de registro das operações de tratamento de dados pessoais pelo responsável ou pelo operador criado pela lei deve prever exceções a casos em que haja risco de identificação de atividades, opções e preferências do titular com as quais não tenha consentido.

"O artigo 40 deve excluir expressamente a obrigatoriedade de registro nos casos em que houver risco de identificação de atividades, opções, preferências e outros aspectos da privacidade e intimidade do titular, nas situações nas quais ele não tenha consentido com o referido registro. Tal como posto, o artigo pode implicar em excessiva intervenção na esfera de privacidade do titular. A não obrigatoriedade do registro nos casos acima expostos busca respeitar a intimidade e os limites do consentimento dado pelo titular.

Ademais, deve-se estabelecer de forma expressa um prazo máximo de manutenção dos registros, a semelhança do que ocorre no MCI quanto a guarda de registros de conexão e acesso a aplicações. Busca-se com isso, novamente, assegurar a inviolabilidade da privacidade e intimidade do titular dos dados".

Autores da proposta: *ABDTIC.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 40. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Autor da sugestão: *GSMA.*

[MODIFICAÇÃO] Art. 40. O responsável ou o operador devem manter, pelo prazo de 1 (um) ano, registro das interações realizadas no tratamento de dados pessoais, incluindo: leitura, alteração, inclusão, exclusão, print da tela, entre outros, observado o disposto do art.15.

4.37.1. Poderes do órgão competente sobre o registro das operações de tratamento de dados pessoais

Respostas controversas coletadas na plataforma de debate:

(A) O órgão competente para a aplicação da lei de proteção de dados pessoais deve ter atribuição legal de poderes para dispor sobre o formato, a estrutura e o tempo de guarda dos registros das operações de tratamento de dados pessoais.

Participantes defendem que a manutenção deste tipo de registro seria de grande importância para a transparência e monitoramento das operações de tratamento de dados. Sendo assim, a elaboração dos critérios para essa guarda não poderia ficar a cargo de cada instância da administração pública ou entidade privada.

Autores da proposta: *Veridiana/Intervozes, Proteste, Luiz Perin Filho.*

(B) A lei não deve regular sobre os formatos de entrega e de guarda dos registros das operações de tratamento de dados pessoais.

"Lei de se abster de regular os formatos de entrega dos da guarda de registro, limitando-se a dispor sobre a obrigação em questão. Isso porque a eleição de um formato em específico desestimula a inovação e a competição, um fornecedor pode, por exemplo, fornecer melhor acesso como um diferencial. A regulação do formato acarretaria engessamento e consistiria em superregulação do tema". (*ABRANET*)

"Este parágrafo deve ser excluído , na medida em que faculta ao órgão competente a criação de mecanismos de controle sem uma clara definição, em âmbito da Lei, de parâmetros e limites para a sua implementação. Tal redação poderia levar a uma má interpretação no sentido de permitir que o órgão competente viesse a criar novas obrigações que apenas o legislador poderia estabelecer, exacerbando o escopo regulador que deve nortear a atuação do órgão". (*Brasscom*)

Autores da proposta: *ABRANET, SindiTeleBrasil, GSMA, Vivo* e *Brasscom.*

(C) Deve ser estabelecido em lei o formato e o tempo de guarda dos registros de operações de tratamento de dados pessoais.

Autores da proposta: *ITI e MPA.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. 40. ~~O responsável ou o operador devem manter registro das operações de tratamento~~ A comunicação de dados pessoais ~~que realizarem, observado o disposto no art. 15.~~ entre responsáveis ou operadores de direito privado dependerá do consentimento do titular, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

~~**Parágrafo único.** Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.~~

4.38. Encarregado pelo tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Seção III – Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.

§ 2º As atividades do encarregado consistem em:

I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações do órgão competente e adotar providências;

III – orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – demais atribuições estabelecidas em normas complementares ou determinadas pelo responsável.

> **§ 3º** Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.

Conforme definido pelo próprio anteprojeto em seu artigo 5º, o encarregado é a pessoa que atua como canal de comunicação entre o responsável e os titulares de dados pessoais e o órgão competente.

Todos os participantes da consulta entendem a importância desse canal de comunicação, no entanto, como se verá abaixo, há algumas opiniões divergentes principalmente quanto à amplitude da atuação deste encarregado dentro de um mesmo grupo econômico e quanto às possíveis hipóteses de dispensa da obrigação de indicar um encarregado no caso, por exemplo, das empresas de pequeno porte.

4.38.1. Qual deve ser o escopo das atribuições do encarregado pelo tratamento de dados pessoais?

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer que poderá haver a nomeação de um encarregado pelo tratamento de dados pessoais que responda pelo grupo econômico como um todo.

"Propomos nova redação tendo em vista que a redação atual do APL leva a crer que deverá existir um funcionário exclusivamente alocado para a função de encarregado dos dados pessoais, este tipo de previsão nem mesmo encontra paralelo na legislação europeia.

A lei deverá dispor sobre a possibilidade de indicação de um único encarregado, dentre os funcionários com função de gestão ou direção já existentes na entidade privada, pelo tratamento de dados dentro de um mesmo grupo econômico ou entidade de classe. Este funcionário deverá poder acumular sua função como encarregado dos dados pessoais com suas antigas funções no ente privado". (*CNseg*)

Autores da proposta: *ITI* e *CNseg* (defende também que deve haver permissão expressa ao acúmulo de funções anteriores).

4.38.2. Hipóteses de dispensa no dever de indicação de um encarregado pelo tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve apenas criar uma opção de indicação de um encarregado pelo tratamento de

dados.

"A exigência de indicação de um encarregado, com atribuição, inclusive, de receber reclamações dos titulares, não leva em conta o volume de demandas dessa natureza recebidas por empresas de grande porte. A disposição, portanto, tal como consta no APL, não melhora o atendimento do titular, apenas o torna mais inviável ou ineficaz".

Autor da proposta: *ABDTIC.*

(B) A lei deve positivar as hipóteses de dispensa de indicação de um encarregado pelo tratamento de dados pessoais e não transmitir essa atribuição ao órgão competente.

"Dessa forma, evita-se que todo e qualquer responsável por tratamento de dados seja obrigado a indicar um encarregado até que o órgão competente crie regulamento acerca das hipóteses de dispensa".

Autor da proposta: *CNseg.*

(C) A lei deve prever a dispensa da obrigação de indicar um encarregado pelo tratamento de dados pessoais, segundo critérios de natureza ou porte da entidade e de volume de operações de tratamento.

Autores da proposta: *SindiTeleBrasil* e *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 41. Órgão competente estabelecerá normas complementares sobre as atribuições do encarregado, inclusive hipóteses da necessidade de sua indicação, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 41. O responsável deverá indicar pessoa natural ou área funcional, que atuará em seu nome, conforme disposto nesta Lei, que atuará como encarregado pelo tratamento de dados pessoais.

Autor da sugestão: *CNseg.*

[INCLUSÃO] 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.

4.38.3. Dever de informação da identidade e contato do encarregado

Todos os participantes que comentaram este parágrafo argumentaram contra a necessidade de divulgação da identidade do encarregado, no entanto, os participantes criticaram esse ponto por motivos diferentes.

A *Câmara BR* e a *ABRANET* argumentaram que a divulgação não poderia ser feita por motivos de segurança e que a lei deveria dispor sobre formas alternativas de contato com o encarregado.

Já a *Fiesp* defendeu que o "encarregado" não deveria ser uma pessoa física, mas sim um departamento responsável pela comunicação com os titulares e com o órgão competente; assim, não seria necessária a identificação da pessoa natural.

Por fim, o *ITI* apontou a simples desnecessidade de identificação do encarregado, sendo o bastante para os fins da norma que o nome do cargo e/ou o nome da posição em conjunto com as informações de contato do referido cargo e/ou posição fossem divulgados.

4.38.4. Atividades do encarregado pelo tratamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei não deve definir as atividades do encarregado pelo tratamento de dados pessoais.

"Acreditamos que esse parágrafo diminui a liberdade das empresas de se organizarem de acordo com o seu modelo de negócio, considerando que, dependendo do tipo de negócio, a função do

encarregado pode mudar".

Autor da proposta: *Câmara BR.*

(B) A lei não deve atribuir, ao encarregado pelo tratamento de dados pessoais, a atividade de receber comunicações do órgão competente.

Autores da proposta: *GSMA, Vivo e SindiTeleBrasil* (contrários à criação de um órgão competente).

(C) A lei deve determinar que as demais atribuições do encarregado pelo tratamento de dados pessoais que forem estabelecidas em normas complementares deverão respeitar a diversidade de atividades e de formas de organização de empresas, considerando o porte, a estrutura e as funções da empresa e a natureza das informações.

Autores da proposta: *ITI* e *MPA* (específico para empresas de pequeno e médio porte).

(D) A lei não deve estabelecer atividades obrigatórias dos encarregados pelo tratamento de dados pessoais, apenas diretrizes.

Autor da proposta: *ABRANET.*

(E) A lei deve prever um regime para a figura do encarregado durante o período entre a sua entrada em vigor e a vigência de normas complementares que regulamentam sua função.

Autor da proposta: *ITI.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Seção ~~III~~ II – Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.

§ 2º As atividades do encarregado consistem em:

I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações do órgão competente e adotar providências;

III – orientar os funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – demais atribuições determinadas pelo responsável ou estabelecidas em normas complementares ~~ou determinadas pelo responsável~~.

§ 3º ~~Órgão~~ O órgão competente ~~estabelecerá~~ poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de ~~definição~~ sua indicação, conforme ~~critérios de~~ a natureza ~~ou~~ e porte da entidade~~, e~~ ou volume de operações de tratamento de dados.

4.39. Segurança e sigilo dos dados pessoais.

REDAÇÃO LEVADA A DEBATE

Seção IV – Segurança e Sigilo dos Dados

Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

4.39.1. As medidas de segurança devem ser constantemente atualizadas e compatíveis com o atual estado da tecnologia?

Propostas avulsas para a regulação deste tema:
(A) Não. A lei deve exigir apenas que as medidas de segurança adotadas sejam adequadas e proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais.

Autores da proposta: *Brasscom, Claro, MPA, ITI, SindiTeleBrasil, Febraban, ABDTIC* e *Sky.*

Sugestões de redação:

Autor da sugestão: *ABA.*

[MODIFICAÇÃO] Art. 42. O operador deve avaliar periodicamente suas medidas de segurança técnicas e administrativas e implementar medidas de segurança técnica e administrativa constantemente atualizadas, sempre que necessário, proporcionais à natureza da informação processada e capaz de proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 42. O responsável deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão ou qualquer outra forma de tratamento inadequado ou ilícito.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único. As medidas de segurança devem ser compatíveis com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

Autor da sugestão: *GPoPAI.*

[INCLUSÃO] § 2º O operador deverá levar em consideração, durante todo o tratamento dos dados pessoais, os direitos e obrigações previstos nessa lei, implementando medidas técnicas organizacionais concebidas para a proteção dos dados pessoais.

§ 3º O órgão competente irá estabelecer os padrões técnicos mínimos para tornar aplicável o quanto disposto no parágrafo anterior, levando-se em consideração desde a fase de concepção do produto ou serviço até a sua execução.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Seção ~~IV~~ **III** – ~~Segurança~~ **Responsabilidade** e ~~Sigilo dos Dados~~ **Ressarcimento de Danos**

Art. 42. Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo.

Parágrafo único. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Art. 43. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.

CAPÍTULO VII - SEGURANÇA E BOAS PRÁTICAS

Seção I - Segurança e Sigilo de Dados

Art. 45. O operador deve adotar medidas de segurança técnicas e administrativas ~~constantemente atualizadas, proporcionais à natureza das informações tratadas e~~ aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação~~, difusão,~~ ou qualquer forma de tratamento inadequado ou ilícito.

~~Parágrafo único. As medidas de segurança devem ser compatíveis com.~~

§ 1º O órgão competente poderá dispor sobre padrões técnicos e organizacionais para tornar aplicável o ~~atual estado da tecnologia~~ disposto no

caput, ~~com~~ levando-se em consideração a natureza ~~dos dados e com as~~ das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis.

§ 2º As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou serviço até a sua execução.

4.40. Dever de sigilo dos agentes de tratamento de dados pessoais.

REDAÇÃO LEVADA A DEBATE

Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve determinar um dever de sigilo aos agentes ou terceiros em contato com o tratamento de dados pessoais, mas estabelecer que eles devam respeitar os limites do consentimento obtido.

"O dever de sigilo é um caso particular que se aplica a determinados tipos de dados e consentimentos. Nesse sentido, ele deve ser compatível com os termos de consentimento estabelecidos no ato da informação dos dados pessoais".

Autor da proposta: *Brasscom.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de respeitar os limites do consentimento obtido no ato da informação dos dados pessoais, quando aplicável, mesmo após o seu término.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~43~~. **46.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

4.41. Comunicação de incidentes de segurança que possam acarretar prejuízos aos titulares de dados pessoais.

REDAÇÃO LEVADA A DEBATE

Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Parágrafo único. A comunicação deverá mencionar, no mínimo:

I – descrição da natureza dos dados pessoais afetados;

II – informações sobre os titulares envolvidos;

III – indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV – riscos relacionados ao incidente; e

V – medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

4.41.1. Como deve ser feita a comunicação, entre o responsável e o órgão competente, sobre incidentes de segurança que possam acarretar prejuízo aos titulares?

Respostas controversas coletadas na plataforma de debate:

(A) Imediata.

"A lei deve estabelecer que a comunicação acerca do incidente seja imediata, mas também deve determinar prazo razoável para o fornecimento de informações adicionais que eventualmente não possam ser apresentadas de imediato".

Quem defendeu isso? *ABDTIC*.

(B) Não imediata, mas com prazo determinado.

Quem defendeu isso? *Câmara Br, Brasscom, MPA, Febraban, Fiesp* e *BSA.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] Art. 44. O responsável deverá comunicar ao órgão competente, assim que o controlador determinar se o incidente pode representar um risco, a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] Art. 44. O responsável deverá comunicar em prazo razoável, de acordo com a proporção do incidente, ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Autor da sugestão: *MPA.*

[MODIFICAÇÃO] Art. 44. O responsável deverá comunicar os indivíduos afetados tão logo possível, dentro de um período razoável de tempo e sem atrasos injustificados, caso seus dados sensíveis tenham sido obtidos por pessoas não autorizadas e tal obtenção possa acarretar prejuízo aos titulares, inclusive financeiro.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 44. O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~44~~ 47. O responsável deverá comunicar ~~imediatamente~~ ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável e deverá mencionar, no mínimo:

I – descrição da natureza dos dados pessoais afetados;

II – informações sobre os titulares envolvidos;

III – indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV – riscos relacionados ao incidente; ~~e~~

V – no caso da comunicação não ter sido imediata, os motivos da demora; e

VI –medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

4.42. Determinação de adoção de providências quanto a incidentes de segurança relacionados a dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:

I – pronta comunicação aos titulares;

II – ampla divulgação do fato em meios de comunicação; ou

III – medidas para reverter ou mitigar os efeitos de prejuízo.

§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.

§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve estabelecer obrigação de qualquer providência quanto a incidentes de segurança relacionados a dados pessoais.

Autores da proposta: *GSMA, Claro, Vivo e SindiTeleBrasil.*

(B) A lei deve estabelecer que a comunicação aos titulares de dados pessoais somente deve ser determinada em casos de risco significativo de roubo de identidade ou de prejuízos financeiros.

Autor da proposta: *ITI.*

(C) A lei deve determinar a necessidade de proteção visual de dados pessoais.

Autor da proposta: *3M do Brasil.*

4.42.1. Pronta comunicação aos titulares de incidentes de segurança relacionados a seus dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei deve estipular um prazo para que empresas que sofreram violação na sua segurança possam investigar e fazer um plano de ação para lidar com o incidente da melhor forma para o consumidor.

Autores da proposta: *Câmara BR e ITI.*

(B) A lei deve estipular critérios para que seja determinada a pronta comunicação aos titulares de incidentes de segurança relacionados a seus dados pessoais.

"Deve haver melhor delimitação da pronta comunicação aos titulares, deixando claro os casos em que ela é efetivamente necessária".

Autor da proposta: *Associação da Liberdade Religiosa e Negócios.*

Sugestões de redação:

Autor da sugestão: *Associação da Liberdade Religiosa e Negócios.*

[MODIFICAÇÃO] I - pronta comunicação aos titulares, em caso de incidentes de segurança envolvendo dados pessoais sensíveis ou quando, após análise pelo órgão competente, for

constatada a efetiva possibilidade de prejuízo aos titulares;

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~45~~ 48. ~~Órgão~~ O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de outras providências ~~quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade~~, tais como:

I – pronta comunicação aos titulares;

II – ampla divulgação do fato em meios de comunicação; ~~ou~~ e

III – medidas para reverter ou mitigar os efeitos ~~de prejuízo~~ do incidente.

§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.

§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos

4.43. Obrigações direcionadas aos sistemas utilizados para o tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Propostas avulsas para a regulação deste tema:

(A) A lei deve prever que os requisitos de segurança a serem atendidos por sistemas de tratamento de dados pessoais devem ser flexíveis e adaptáveis a entidades diferentes em estrutura, porte e tipo de informações tratadas.

Autor da proposta: *ITI.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~46.~~ 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

4.44. Poder normativo do órgão competente quanto a critérios e padrões mínimos de segurança

REDAÇÃO LEVADA A DEBATE

Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve conferir poder normativo acerca de critérios e padrões mínimos de segurança ao órgão competente.

Autores da proposta: *GSMA, SindiTeleBrasil, Vivo.*

(B) A lei deve estabelecer a obrigação de realização de auditoria independente nos sistemas de segurança de forma periódica.

"A lei poderia especificar órgãos responsáveis por realizar auditorias independentes nos sistemas de segurança de forma periódica, estabelecendo, conforme a natureza dos dados e da atividade da empresa auditada, pelo menos uma auditoria por ano ou por outro prazo necessário".

Autor da proposta: *RafaelC.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 47.** Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.~~

4.45. Boas práticas no tratamento de dados pessoais

REDAÇÃO LEVADA A DEBATE

Seção V – Boas Práticas

Art. 48. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados.

Parágrafo único. As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve dispor sobre a possibilidade de boas práticas no tratamento de dados pessoais.

Para os participantes que defendem essa posição seria evidente que, desde que respeitadas as obrigações legais, os responsáveis poderão se organizar da maneira que preferirem.

Autores da proposta: *Claro, SindiTeleBrasil* e *Felipe Ivanoff.*

(B) A lei deve incluir a menção à educação digital associada a boas práticas.

"A criação e divulgação de melhores práticas e o incentivo a educação digital é essencial para evitar a propagação de golpes na internet, sendo assim, propomos nova redação de forma a privilegiar estes importantes aspectos".

Autor da proposta: *Fiesp.*

(C) A lei deve estabelecer que a formulação e adoção de boas práticas pode servir como mecanismo de permissão de transferência internacional de dados pessoais, caso as mesmas práticas forem adotadas pelas organizações em outras jurisdições.

Autor da proposta: *ITI.*

(D) A lei deve criar normas mínimas de segurança associadas ao fomento de boas práticas.

"O artigo deveria prever normas mínimas de segurança a serem seguidas. No que tange as normas de segurança, acredito que seja inviável deixar o artigo de foram tão abstrata, acredito que este aspecto deva ser impositivo, trazendo no seu escopo diretrizes mínimas para aqueles que se dispuserem a realizar a guarda de dado alheios, assim poderia fazer uma seleção natural dos profissionais bem como empresas qualificadas para exercer tão atividade".

Autor da proposta: *Josimar.*

(E) A lei deve prever mecanismos de incentivo à formulação de boas práticas e que estas sejam aplicáveis tanto a responsáveis como a operadores de tratamento de dados pessoais.

Participantes defendem que a lei deve:

(1) Prever a aplicação das regras de boas práticas a todos os elementos da "responsabilização organizacional";

(2) Enfatizar o papel central da privacidade nas boas práticas de gestão de risco;

(3) Estabelecer incentivos para que as empresas participem ou formulem regras de boas práticas (*ABDTIC*); e

(4) Ressaltar sua aplicação tanto a responsáveis quanto a operadores do tratamento de dados.

Autores da proposta: *ABDTIC* e *Centre for Information Policy Leadership.*

Sugestões de redação:

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] Art. 48. O órgão competente e os demais envolvidos no tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados, além do incentivo à educação digital para a prevenção de eventuais riscos.

Autor da sugestão: *Centre for Information Policy Leadership.*

[MODIFICAÇÃO] Art. 48. Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos.

4.45.1. Reconhecimento e divulgação de boas práticas por parte do órgão competente

Os participantes se dividiram entre duas posições quanto à possibilidade de reconhecimento e divulgação de boas práticas por parte do órgão competente.

A primeira posição foi adotada pela *ABEP* e pela *GSMA,* que pediram a exclusão de tal possibilidade. Dentre os motivos apresentados, a *ABEP* apontou a falta de clareza em relação à força normativa das regras de boas práticas uma vez divulgadas. Segundo a associação, restrições como esta devem ser estabelecidas através do Poder Legislativo ou do órgão competente.

Já os participantes *Marcus Lage Pinto*, *Jacqueline Abreu* e *Prof. Marcos* sugeriram a troca do termo "poderão" por "deverão", ou seja, argumentaram pela obrigatoriedade do reconhecimento e divulgação das regras pelo órgão competente. Segundo os participantes, o órgão competente deve realizar um papel orientador das boas práticas no sentido de fomentar sua atualização e alinhamento com o "estado do tecnologia".

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Seção ~~V~~ II – Boas Práticas

Art. ~~48~~ 50. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas

para os diversos envolvidos no tratamento, ações ~~formativas ou~~ **educativas**, mecanismos internos de supervisão e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, ~~observado~~ o ~~disposto nesta Lei~~ responsável pelo tratamento e o operador levarão em ~~normas complementares sobre proteção de~~ consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos.

~~Parágrafo único.~~ **§ 2º** As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.

4.46. Estímulo à adoção de padrões técnicos que facilitem a disposição dos titulares sobre seus dados

REDAÇÃO LEVADA A DEBATE

Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento.

Propostas avulsas para a regulação deste tema:

(A) A lei não deve dispor sobre estímulos à adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais.

Participantes afirmam que tais estímulos tratam de condicionantes desnecessários à lei e que são contrários à criação do órgão competente.

Autores da proposta: *GSMA, Vivo, Claro, SindiTeleBrasil, Brasscom, Câmara BR, ABDTIC e ABRANET.*

(B) A lei deve delimitar o termo "rastreamento", atribuindo ao titular de dados pessoais a capacidade de autorizar ou não seu rastreamento através do consentimento.

Segundo os defensores dessa proposta, o rastreamento, em vários casos, pode ser parte integrante de um serviço e o que possibilita a prestação de determinados serviços.

Autores da proposta: *ITI, ABEP e Fiesp.*

Sugestões de redação:
Autor da sugestão: *ABEP.* **[MODIFICAÇÃO]** Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento não autorizado pelo titular.
Autor da sugestão: *Fiesp.* **[MODIFICAÇÃO]** Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais.
Autor da sugestão: *Brasscom.* **[MODIFICAÇÃO]** Art. 49. Os agentes econômicos poderão adotar padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais.
Autor da sugestão: *American Bar Association.* **[INCLUSÃO]** Parágrafo único. Órgão competente deverá estabelecer regras e padrões complementares para as medidas de dissociação de dados pessoais (por anonimização ou por desidentificação), os quais deverão estar em conformidade com os princípios gerais de proteção dos dados e direitos dos titulares.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

Art. ~~49~~ 51. O órgão competente estimulará a adoção de padrões técnicos ~~para softwares e aplicações de Internet~~ que facilitem ~~a disposição~~ o controle dos titulares sobre seus dados pessoais~~, incluindo o direito ao não rastreamento.~~

4.47. Sanções administrativas

REDAÇÃO LEVADA A DEBATE

CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS

Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:

I – multa simples ou diária;

II – publicização da infração;

III – dissociação dos dados pessoais;

IV – bloqueio dos dados pessoais;

V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;

VI – cancelamento dos dados pessoais;

VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e

VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.

§ 1º As sanções poderão ser aplicadas cumulativamente.

§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.

§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

Com relação às sanções administrativas previstas no *caput* e nos incisos do artigo 5º, as contribuições, para melhor sistematização, foram divididas em cinco conjuntos: (i) contribuições de caráter geral acerca das sanções; (ii) contribuições acerca da multa (inciso I); (iii) contribuições sobre publicização da infração (inciso II); (iv) contribuições sobre a obrigação de

dissociação, bloqueio e cancelamento (incisos III, IV e VI); e, por fim, (v) contribuições sobre sanções que envolvem proibição ou suspensão do tratamento de dados ou do funcionamento dos bancos de dados (incisos V, VII e VIII).

Cabe ainda ressaltar que as sanções previstas nesse artigo não causam prejuízo a outras consequências de natureza civil ou penal, ou seja, eventuais indenizações aos titulares de dados e responsabilizações pessoais das pessoas envolvidas no tratamento de dados não são afastadas pelo previsto neste artigo.

4.47.1. Propostas gerais sobre sanções administrativas

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar mecanismos e procedimentos para que a aplicação das sanções administrativas atendam ao contraditório, à ampla defesa e ao devido processo legal.

Autores da proposta: *Vivo, Febraban e Jhonata Goulart Serafim.*

(B) A lei deve estabelecer que as sanções administrativas sejam proporcionais ao risco que a violação da qual elas decorrem pode causar aos consumidores, bem como atendam aos princípios da Administração Pública.

Autores da proposta: *SindiTeleBrasil* (também sugere a inclusão da "advertência" como sanção possível), *Cisco* e *Claro.*

(C) A lei deve determinar que sua execução ficará a cargo de somente um órgão.

"*Ressalta-se que a execução desta lei deve caber a um só órgão, de forma a evitar inconsistência e duplicidade de esforços*".

Autores da proposta: *ITI.*

(D) A lei deve criar sanções penais para casos graves, de abrangência coletiva ou de reincidência infracional.

Autores da proposta: *Marcus Lage Pinto, Anderson, Prof. Marcos, Bernado Kahl, Luiz Fernando Borges e Tibério Sampaio* (propões sanções mais gravosas em casos de reincidência).

Sugestões de redação:

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às

normas previstas nesta Lei ficam sujeitas às sanções administrativas a seguir estabelecidas e que devem ser aplicadas de forma gradativa.

Autor da sugestão: *Febraban.*

[MODIFICAÇÃO] Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente, resguardado o direito ao contraditório e à ampla defesa.

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas, após a instauração do respectivo processo administrativo sancionador.

4.47.2. Propostas sobre multa simples ou diária

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer um limite máximo para a multa.

Os participantes que defenderam essa proposta acreditam que ela impedirá que o valor da multa diária acumulada ultrapasse limites razoáveis.

Autores da proposta: *Câmara BR, Brasscom, ITI, CNseg, ABINEE, ABRANET* e *Cassia.*

(B) A lei não deve trazer previsão de multa diária.

"Sugere-se retirada da previsão de multa diária em atendimento ao princípio da razoabilidade. A determinação de multa diária mostra-se desproporcional se não levado em conta o nível da infração praticada, podendo resultar em um valor de grande monta que venha a causar prejuízo à atividade profissional desenvolvida pelo responsável".

Autor da proposta: *Febraban.*

(C) A lei deve prever uma etapa de notificação ao responsável pelo tratamento de dados pessoais anterior à aplicação de sanção. A sanção só deverá poder ser aplicada se não houver atendimento à determinação contida na notificação.

"Lei deve determinar que seja feita notificação ao responsável pelo tratamento de dados por parte da autoridade competente antes de se aplicar a sanção.

Diversas leis de proteção de dados, como a Francesa, 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".

Autor da proposta: *CNseg.*

(D) A lei deve determinar que o montante arrecadado pelas multas seja revertido ao órgão competente.

"Mostra-se interessante especificar ao que se destinarão os valores recebidos com a arrecadação provinda das multas. Seria satisfatório se estes valores serão revertidos ao órgão ou entidade responsável pela fiscalização para que este se aperfeiçoe constantemente, pois a tecnologia é algo em constante avanço e uma lei como essa só tem eficácia com a devida fiscalização técnica. O uso de dados ainda gera grande insegurança e ter um órgão fiscalizador bem equipado e atualizado traz segurança".

Autora da proposta: *Cassia.*

4.47.3. Propostas sobre sanção de publicização da infração

Propostas avulsas para a regulação deste tema:

(A) A lei deve determinar que a publicização de qualquer infração não poderá ocorrer até a sua determinação definitiva, garantido o direito de recurso contra atos do órgão competente.

Autores da proposta: *Câmara BR e ITI.*

(B) A lei deve estabelecer a publicização das infrações como consequência da aplicação das sanções administrativas, e não como uma sanção específica.

"Publicização da infração não deveria ser uma forma de sanção administrativa e sim consequência da aplicação das sanções em virtude do Princípio da Publicidade dos atos. De que forma efetivamente a publicidade da infração seria uma forma de sanção? Penso que sanções devem ser rígidas, pois se trata de informações e dados pessoais, e a sanção do inciso II não enquadra nesse aspecto".

Autora da proposta: *Jéssica Lustrosa.*

4.47.4. Propostas sobre sanções que determinem dissociação, bloqueio ou cancelamento de dados pessoais

Propostas avulsas para a regulação deste tema:

(A) A lei não deve prever sanções que determinem: (i) dissociação, (ii) bloqueio ou (iii)

cancelamento de dados pessoais.

"Este tipo de sanção (...) *pode limitar, ou mesmo inviabilizar, as atividades das organizações e, portanto, indisponibilizar o serviço aos consumidores".* (*ITI*)

"Os termo 'bloqueio' e 'cancelamento' são vagos e implicam na impossibilidade da livre realização de atividade econômica. Sugerimos, portanto a retirada dos incisos IV e VI, sob pena de ser objeto de questionamento". (*ABDTIC*)

"(N)ão é recomendado atribuir ao Órgão Competente, sem expressão de vontade do titular, a determinação de cancelamento de dados pessoais, uma vez que eventual interesse do titular em manter relacionamento com determinada empresa pode ser frustrado em razão da sanção administrativa imposta". (*Febraban*)

Autores da proposta: *ITI* (**i**, **iii** e **iii**), *ABDTIC* (**ii** e **iii**), *Cisco* (somente **iii**), *Febraban* (somente **iii**).

(B) A lei deve prever que a sanção que determine dissociação de dados pessoais seja limitada aos dados relativos à infração e ao ínterim percebido até regularização da situação.

"O inciso III deve prever que a dissociação deve ser limitada aos dados pessoais relativos à infração e limitada ao ínterim percebido até sua regularização. Isso porque não há vantagem, nem mesmo ao titular, em manter esta situação indefinidamente, já que o tratamento de seus dados pessoais, por estarem dissociados, poderá restar prejudicado".

Autor da proposta: *Febraban.*

(C) A lei deve prever uma sanção que determine a anonimização de dados pessoais, em lugar do termo "dissociação".

Autores da proposta: *Veridiana/Intervozes e Proteste.*

4.47.5. Sanções que determinem a suspensão de operação de tratamento de dados pessoais ou proibição de tratamento de dados sensíveis ou de funcionamento de banco de dados

Propostas avulsas para a regulação deste tema:

(A) A lei não deve prever sanções que determinem a suspensão de operação de tratamento de dados pessoais ou proibição de tratamento de dados sensíveis ou de funcionamento de banco de dados.

Participantes defendem que tais sanções inviabilizam a operação de empresas que dependem do tratamento de dados para operar.

Autores da proposta: *ABEMD, ITI, Câmara BR, ABDTIC, Cisco, Brasscom* e *MPA.*

(B) A lei deve estabelecer que sanções de suspensão ou proibição ligadas ao tratamento de

dados pessoais devam vigorar até que sejam sanadas as irregularidades.

"Os prazos de que falam os incisos do artigo devem ser todos alterados para o prazo indeterminado 'até que sanadas as irregularidades'. De forma a adequar o prazo da sanção administrativa com o tempo pelo qual a infração causa danos aos usuários".

Autor da proposta: *ABEP.*

(C) A lei deve limitar o escopo das sanções de suspensão ou proibição ligadas ao tratamento de dados pessoais.

"Os incisos V e VII devem ser alterados de forma a afetar somente os dados pessoais atingidos e, além disso, é necessário diminuir o prazo de 10 anos. Quanto ao inciso VIII, este deve ser excluído, posto que a proibição de funcionamento de banco de dados tem o mesmo efeito das penalidades já tratadas nos demais incisos, que podem ser aplicados cumulativamente".

Autor da proposta: *Febraban.*

4.47.6. Aplicação cumulativa de sanções

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer que a aplicação cumulativa de sanções deva ser permitida apenas em caso de reincidência infracional.

Autor da proposta: *ABDTIC.*

(B) A lei deve permitir a aplicação de sanções cumulativamente, desde que não sejam da mesma natureza.

"Sugerimos mudança de redação tendo em vista o objetivo de respeitar o princípio do non bis in idem, que veda a aplicação de múltiplas sanções para uma mesma conduta infratora".

Autor da proposta: *Vivo.*

(C) A lei deve prever que a aplicação cumulativa de sanções deva estar condicionada à proporcionalidade e critérios pré-estabelecidos.

"A proporcionalidade deve ser levada em conta na ocasião da aplicação da sanção. As sanções, portanto, devem ser aplicadas de forma gradativa, reservando-se as sanções mais graves para hipóteses de reincidência. A proteção de dados será melhor garantida por meio de mecanismos de fiscalização com foco no aumento da detecção das violações e do fomento das boas relações de confiança entre indústria e regulador".

Autor da proposta: *Fiesp.*

Sugestões de redação:

Autor da sugestão: *Vivo.*

[MODIFICAÇÃO] §1° As sanções, desde que não sejam de mesma natureza, poderão ser aplicadas cumulativamente.

Autor da sugestão: *Fiesp.*

[MODIFICAÇÃO] §1º O Regulamento estabelecerá os patamares e as condições de aplicação das sanções previstas acima, inclusive as ocasiões em que poderão ser aplicadas cumulativamente.

4.47.7. Procedimentos e critérios para aplicação das sanções administrativas

Propostas avulsas para a regulação deste tema:

(A) A lei deve criar circunstâncias atenuantes à aplicação de sanções, abrindo espaço para qualificadores positivos.

"Lei deve criar também circunstâncias atenuantes à aplicação das sanções. Deve haver espaço para qualificadores positivos, como a existência de um programa abrangente de privacidade, a velocidade de introdução de fatores de correção, a ausência de intencionalidade.

Multas razoáveis são uma parte fundamental de qualquer regime sólido de proteção de dados. No entanto, o dado de que o projeto de lei é aplicável a todos os setores e tamanhos de negócios exige uma abordagem diferenciada e equilibrada. Também é importante para evitar que o elevado nível de sanções possa minar o incentivo das empresas para investir no Brasil e desincentivar a interação das empresas com órgãos reguladores". (*Câmara BR*)

Autores da proposta: *ABRANET e Câmara BR.*

(B) A lei deve estabelecer que a adoção de critérios para aplicação de sanções não poderá prejudicar o agente particular de maneira que lhe cause a inviabilidade do negócio.

Autor da proposta: *Brasscom.*

(C) Somente a lei (e não o regulamento) deve prever procedimentos e critérios para aplicações das sanções nela previstas.

Participantes justificam a posição devido à atenção ao princípio da tipicidade.

Autores da proposta: *Tarso Cabral Violin e Kaliny Aglay.*

Sugestões de redação:

Autor da sugestão: *Brasscom.*

[MODIFICAÇÃO] § 2º Os procedimentos e critérios para a aplicação das sanções respeitarão os princípios da razoabilidade e proporcionalidade e serão adequados em relação à gravidade e à extensão da infração; à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.

4.47.8. Prorrogação de prazos de sanções de proibição pelo órgão competente

Propostas avulsas para a regulação deste tema:

(A) A lei deve estabelecer que sanções de suspensão ou proibição ligadas ao tratamento de dados pessoais devam vigorar até que sejam sanadas as irregularidades[29].

"Os prazos de que falam os incisos do artigo devem ser todos alterados para o prazo indeterminado 'até que sanadas as irregularidades'. De forma a adequar o prazo da sanção administrativa com o tempo pelo qual a infração causa danos aos usuários".

Autor da proposta: *ABEP.*

(B) A lei não deve prever a prorrogação de sanções de proibição pelo órgão competente.

"Sugere-se a eliminação do dispositivo. O dispositivo trata de um poder grande demais para ser dado à administração pública, tal medida, se implementada, acabará por inviabilizar por completo a atividade de determinadas empresas que atuam por meio de modelos de negócios online ou de empresas que trabalham com a guarda registros em data bases.

Nesse cenário, a possibilidade de prorrogação do prazo, já longo, da sanção prevista no § 3° apenas reforça nossa tese de que as margens da sanção estão muito amplas e atribuem poder excessivo ao Poder Administrativo". (*MPA*)

Autores da proposta: *MPA e ITI.*

Sugestões de redação:

Autor da sugestão: *ABEP.*

[MODIFICAÇÃO] § 3º As proibições previstas nos incisos VII e VIII do caput perdurarão enquanto verificada a omissão no cumprimento das determinações do órgão competente, a reincidência no

[29] Mesma proposta do ponto 4.47.5.

cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

Autor da sugestão: *SindiTeleBrasil.*

[MODIFICAÇÃO] § 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, respeitados o limite superior, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

4.47.9. Possibilidade de aplicação de sanções administrativas, civis e penais previstas em legislação específica

Propostas avulsas para a regulação deste tema:

(A) A lei deve conferir a uma autoridade federal única a aplicação de sanções relacionadas ao seu eventual descumprimento.

Autor da proposta: *Brasscom.*

(B) A lei não deve fazer menção a sanções administrativas, já que as penalidades por ela impostas são dessa natureza.

"O parágrafo não deve fazer menção às sanções administrativas já que as penalidade impostas por meio do artigo são administrativas, de forma que não deve cumular com outros de mesma natureza.

Autor da proposta: *Febraban.*

(C) A lei deve vedar expressamente o *bis in idem* na aplicação de sanções administrativas, civis e penais previstas em legislação específica.

Autor da proposta: *Câmara BR.*

Sugestões de redação:

Autor da sugestão: *Câmara BR.*

[MODIFICAÇÃO] § 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica, desde que não implique em bis in idem.

4.47.10. A que sanções os órgãos públicos devem estar sujeitos? Deve haver diferença entre as sanções a agentes privados e públicos?

O anteprojeto nem sempre destina o mesmo tratamento para entidades privadas e públicas. O tratamento diferenciado pode ser visto, por exemplo, na dispensa de consentimento para algumas hipóteses aplicáveis a órgãos públicos. Este tipo de distinção parece conter a intenção de facilitar o cumprimento dos deveres da Administração Pública e a implementação de políticas públicas.

Entretanto, houve debate na plataforma quanto à extensão deste tipo de tratamento diferenciado em relação às sanções administrativas. Como se vê abaixo, as opiniões se diferenciam entre aqueles que acreditam que a maioria das sanções previstas no artigo causaria prejuízo injustificado para a Administração Pública e os que não enxergam motivo para a ausência de paridade nas sanções voltadas aos agentes públicos e privados.

Respostas controversas coletadas na plataforma de debate:

(A) As pessoas jurídicas de direito público devem estar sujeitas a apenas algumas das sanções administrativas previstas na lei.

"*Os órgãos públicos deveriam estar sujeitos apenas às sanções previstas nos incisos II e III. Entendemos que as sanções estabelecidas nos demais incisos, se aplicadas aos órgãos públicos, implicarão em prejuízo injustificado para a administração pública, bem como no comprometimento de atribuições que lhes são peculiares, em prejuízo dos administrados e de políticas públicas*".

Quem defendeu isso? *Proteste*.

(B) As pessoas jurídicas de direito público devem estar sujeitas ao mesmo regime de sanções administrativas aplicável a pessoas jurídicas de direito privado.

Participantes que defendem a paridade no regime de sanções administrativas aplicável a pessoas jurídicas de direito público e privado entendem que a ausência do mesmo tratamento é inconstitucional, já que a Constituição determina que empresas públicas e sociedades de economia mista que exploram atividades econômicas se sujeitarão ao regime jurídico próprio das empresas privadas.

Quem defendeu isso? *ABEMD, Fiesp, ABDTIC* e *Luiz Perin Filho.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

CAPÍTULO VIII – ~~SANÇÕES ADMINISTRATIVAS~~ FISCALIZAÇÃO

Seção I – Sanções Administrativas

Art. ~~50~~ **52**. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis ~~por~~ pelo órgão competente:

I – multa simples ou diária;

II – publicização da infração;

III – ~~dissociação~~ anonimização dos dados pessoais;

IV – bloqueio dos dados pessoais;

V – suspensão de operação de tratamento de dados ~~pessoais, por prazo não superior a dois anos;~~ pessoais**;**

VI – cancelamento dos dados pessoais;

VII – ~~proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e~~

~~VIII – proibição~~ suspensão de funcionamento de banco de dados~~, por prazo não superior a dez anos~~.

§ 1º As sanções ~~poderão ser~~ serão aplicadas fundamentadamente, isolada ou cumulativamente~~. § 2º Os procedimentos~~**,** de acordo com as peculiaridades do caso concreto e ~~critérios para~~ **com** a ~~aplicação das sanções serão adequados em relação à~~ gravidade e ~~à extensão da infração~~ natureza das infrações, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados~~, nos termos do regulamento~~. ~~§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.~~ ~~§ 4º~~

§ 2º O disposto neste artigo não ~~prejudica~~ substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica. ~~§ 5º~~

§ 3º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990**,** e na Lei nº 8.429, de 2 de junho de 1992.

Seção II – Órgão Competente e Conselho Nacional de Proteção de Dados e da Privacidade

Art. 53. O órgão competente designado para zelar pela implementação e fiscalização da presente Lei terá as seguintes atribuições:

I – zelar pela proteção dos dados pessoais, nos termos da legislação;

II – elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;

III – promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança;

IV – promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

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

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

VII – elaborar relatórios anuais acerca de suas atividades;

VIII – editar normas sobre proteção de dados pessoais e privacidade; e

IX – realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação.

Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade contará com quinze representantes titulares e quinze suplentes designados pelo Ministro de Estado da Justiça, com mandato de dois anos, podendo ser renovado uma única vez por igual período, sendo:

I – sete representantes do Poder Executivo Federal, indicados por ato do Poder Executivo;

II – um representante indicado pela Câmara dos Deputados;

III – um representante indicado pelo Senado Federal;

IV – um representante indicado pelo Conselho Nacional de Justiça;

V – um representante indicado pelo Conselho Nacional do Ministério Público;

VI – um representante indicado pelo Comitê Gestor da Internet no Brasil;

VII – um representante da sociedade civil;

VIII – um representante da academia; e

IX – dois representantes do setor privado.

§ 1º A participação no Conselho Nacional será considerada atividade de relevante interesse público, não remunerada.

§ 2º Os representantes referidos no inciso II ao VI do caput e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 3º Os representantes referidos nos incisos VII a IX do caput e seus respectivos suplentes serão indicados, nos termos do regimento interno a ser aprovado posteriormente.

Art. 55. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I – fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III – sugerir ações a serem realizadas pelo órgão competente;

IV – realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e

V – disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.

4.48. Disposições transitórias e finais

REDAÇÃO LEVADA A DEBATE

CAPÍTULO IX – DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 51. Órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento, a natureza dos dados e o porte do responsável.

Para além das propostas abaixo elencadas, neste dispositivo também foram inseridas diversas contribuições de participantes que sentiram falta da definição de qual seria o órgão competente para a aplicação da lei (*Veridiana Alimonti, CNseg, Associação da Liberdade Religiosa e*

Negócios, Centre for Information Policy and Leadership, Ellen Sartori, Margareth e Giovanna Carloni).

Como explicado no início do relatório, o Ministério da Justiça optou por não levar ao debate público um formato jurídico para tal autoridade de garantia.

Propostas avulsas para a regulação deste tema:

(A) A lei deve determinar que normas de transição respeitem relações já estabelecidas, direitos adquiridos e atos jurídicos perfeitos.

Autores da proposta: *Sky*, *ABEMD* e *Febraban.*

(B) A lei deve estabelecer limites mínimo e máximo para a adequação.

Participantes defenderam que tal proposta evitaria que as disposições nunca fossem implementadas ou que ainda o órgão competente impusesse prazo muito curto.

Autores da proposta: *Paulo Rená e Luiz Perin Filho.*

(C) A lei deve estabelecer que a atuação do órgão competente no período de adequação progressiva não passará por exame de bancos de dados.

"Esse artigo necessita de melhores explicações. Essa disposição sugere que os bancos de dados serão examinados, o que não seria apropriado. O exame ou aprovação dos bancos de dados é um ônus administrativo".

Autor da proposta: *ITI.*

(D) A lei não deve criar uma obrigação, mas uma faculdade ao órgão competente de editar normas de adequação progressiva.

Autor da proposta: *Brasscom.*

(E) A lei deve prever que haja interlocução com autoridades estrangeiras.

"Lei deve prever a interlocução com autoridades alienígenas. Esta interlocução deve ter como objetivo a uniformização das práticas acerca da proteção de dados e o controle sobre a vigilância. A uniformização das regras no panorama internacional é de fundamental importância para a inovação realiza pelos edge providers".

Autor da proposta: *Roberto Taufick.*

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi modificado conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

CAPÍTULO IX – DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. ~~51~~ 56. ~~Órgão~~ Esta Lei entrará em vigor no prazo de 180 dias contados da data da sua publicação.

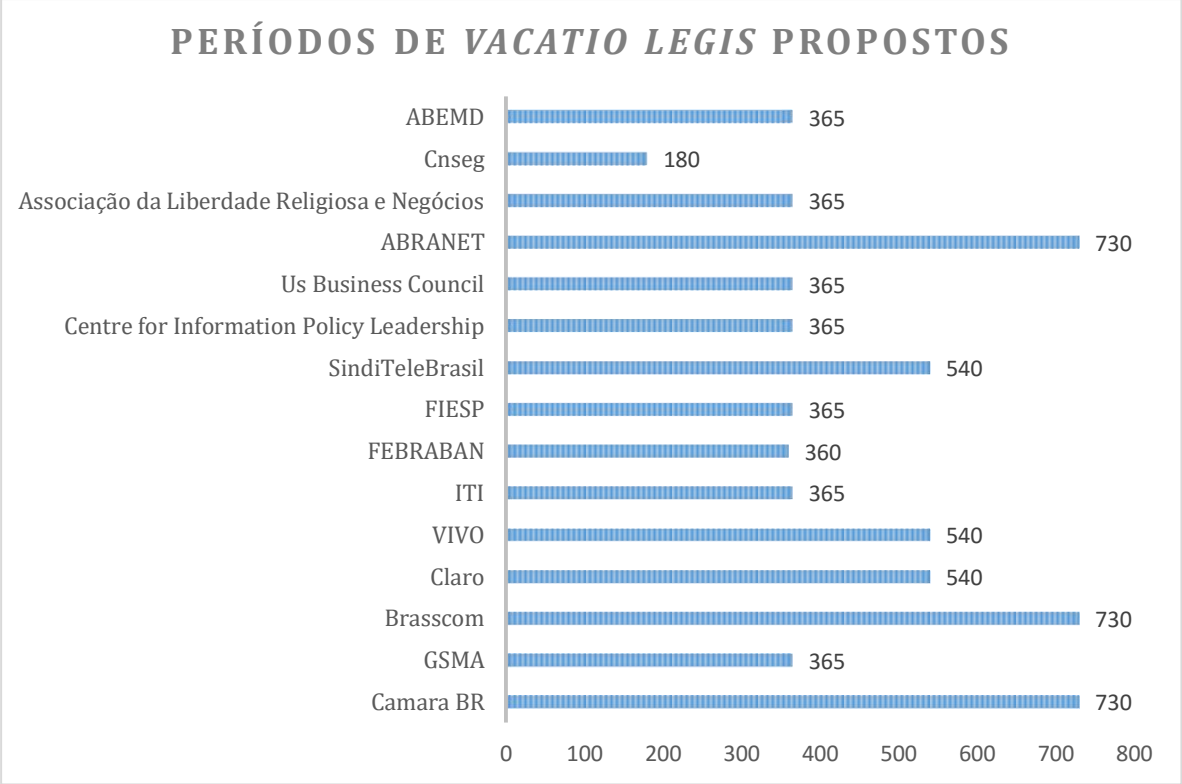
Parágrafo único. O órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento~~,~~ e a natureza dos dados ~~e o porte do responsável.~~

4.49. *Vacatio legis*

REDAÇÃO LEVADA A DEBATE

Art. 52. Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.

Os participantes apresentaram diversas propostas de períodos que seriam adequados para o prazo para a lei entrar em vigor. Visando a organizar essas propostas, elaboramos o gráfico abaixo com os períodos *vacatio legis* sugeridos.



Cabe observar que a *US Business Council* solicitou que a contagem se inicie a partir da criação do órgão competente fiscalizador. Além disso, a *Abranet* sugeriu em um primeiro momento 1 ano de prazo, mas disse que preferencialmente o prazo deveria ser de 2 anos. O *CNseg*, por sua vez, sugeriu que a própria lei, e não a autoridade competente, tratasse de regras transitórias que estabelecessem um prazo para adequação às novas normas para os dados já em funcionamento no momento da entrada da vigor da lei.

Após a compilação das contribuições, a Secretaria Nacional do Consumidor do Ministério da Justiça disponibilizou uma nova versão do anteprojeto de lei. O artigo em debate foi suprimido conforme abaixo:

REDAÇÃO DA VERSÃO DE 20/OUTUBRO/2015

~~**Art. 52.** Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.~~

5. LISTA DE PARTICIPANTES

Participante	Significado da sigla
3M do Brasil	
ABA	Associação Brasileira de Anunciantes
ABDTIC	Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações
ABEMD	Associação Brasileira de Marketing Direto
ABEP	Associação Brasileira de Empresas de Pesquisa
ABINEE	Associação Brasileira da Indústria Elétrica e Eletrônica
ABRANET	Associação Brasileira de Internet
adamir	
Amanda Arrivabene	
Amanda HN	
American Bar Association	Associação dos Advogados Americanos/EUA
Ana Amélia	
Ana Flávia Fagundes Ferreira	
Anderson	
andremenegazzo	
Aparecida Cristina	
Arns	
Associação da Liberdade Religiosa e Negócios	
Bernado Kahl	
Boa Vista Serviços	
Brasscom	Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação
Bruna de Rosa	
Bruno Diego	
Bruno R. Bioni	
BSA	The Business Software Alliance
Câmara BR	Câmara Brasileira de Comércio Eletrônico
Cassia	
Centre for Information Policy Leadership	
Cisco	Cisco Systems, Inc
Claro	
Cláudio Lucena	
CNI	Confederação Nacional da Indústria

CNseg	Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização
CTS-FGV	Centro de Tecnologia e Sociedade da Fundação Getulio Vargas
Daniel Astone	
Danielekfontes	
decko	
Drica	
Eden Grei	
Elen	
Elis	
Elizane Gomes	
ellen sartori	
Emerson Wendt	
ESA	Entertainment Software Association (EUA)
Fabricio Pessôa	
fbraga	
Febraban	Federação Brasileira de Bancos
Felipe de Ivanoff	
FIESP	Federação das Indústrias do Estado de São Paulo
Gabriela Martins	
Gabriele Ferreira	
gabriellebolina	
GEPI-FGV	Grupo de Ensino e Pesquisa em Inovação da Fundação Getulio Vargas
Giovanna Carloni	
Gleison Melo	
GPoPAI	Grupo de Pesquisa em Políticas Públicas de Acesso à Informação
GSMA	Groupe Speciale Mobile Association
IAB	Interactive Advertising Bureau
Inês Barros do Nascimento	
ITI	Instituto Nacional de Tecnologia da Informação
ITS-Rio	Instituto de Tecnologia e Sociedade do Rio de Janeiro
JCK	
Jéssica Brasil	
Jéssica Lustrosa	
Joana Varon	
Josimar	
Kacsavio	
Kaliny Aglay	
Katia Cavalcanti	
Keity Mary Kjhelin Teixeira Vieira	

Kilcy Bispo	
Larissa Denski Nola	
Lucas Zolet	
Luiz Fernando Borges	
Magno	
Maiara de Rosa Freitas	
Marcelo Saldanha	
Márcia P. Soldate	
Marcos Baldin	
Marcus Lage Pinto	
Margareth	
Maria Cunha de Melo	
Mariana Cunha e Melo	
Maurício Coeli	
MPA	
MVianna	
Náthaly Morgani	
Névoa	
Nicole Oliveira	
Paulo C.A.	
Privacy International	
Prof. Marcos	
Proteste	Associação Brasileira de Defesa do Consumidor
Rafaela 16	
RafaelC.	
Raissa Guimarães	
RELX Group	
Roberto Taufick	
Rodrigo	
Rodrigo Junqueira	
Rodrigo Veleda	
RubemRJ	
SEAE/MF	Secretaria de Acompanhamento Econômico do Ministério da Fazenda
SindiTeleBrasil	Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal
Sky	
Stefan	
Tagwato	
Tarso Cabral Violin	
Tássia Martins	
Tatiane Ferreira	

Thiago	
Tibério Sampaio	
TV Aberta	
TV Aberta + Merchant = Peculato	
US Business Council	Brazil-U.S. Business Council
Veridiana/Intervozes	Veridiana Alimonti, do Intervozes
Vivo	
Wagner Silveira	
Wellington Cremasco	