São Paulo, 05 de julho de 2015.

Ao
Excelentíssimo Senhor José Eduardo Cardozo
Ministro da Justiça

C/C:

Mariana Giostri Oliveira Rolim, Diretora Executiva, Brasscom
Sergio Sgobbi, Diretor de Relações Institucionais, Brasscom

Assunto: Consulta pública sobre o Anteprojeto de Lei de Proteção de Dados Pessoais

Prezado Sr. José Eduardo Cardozo,

A missão da Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, é aumentar a competitividade global do setor de TIC do Brasil e disseminar a sua capacidade transformadora para todos os outros setores econômicos, aumentando a sua eficiência e produtividade e criando benefícios para toda a sociedade brasileira.

Ao longo dos últimos meses, a Brasscom desenvolveu amplos debates e ouviu seus associados sobre os dispositivos propostos no referido Anteprojeto de Lei, objetivando recomendações concretas que sejam compatíveis com o texto e alinhadas com o futuro, no tocante à inovação e ao desenvolvimento do setor e da economia digital.

Sendo o que nos cumpria para o momento, colocamo-nos à disposição para o que for necessário e aproveitamos a oportunidade para externar nossos protestos de estima e consideração.

Cordialmente,

Sergio Paulo Gallindo
Presidente Executivo

Associação Brasileira das Empresas
de Tecnologia da Informação e Comunicação

Associados da Brasscom

A Brasscom tem 38 associados dentre as maiores e mais significativas empresas do setor e conta com 10 associados institucionais.

São associados da Brasscom: Accenture, Algar Tech, Apple, Atos, BRQ, Capgemini, CI&T, Cisco, Dell, EMC^2, Equinix, Facebook, GFT, Globalweb, Google, Grupo Contax, HP, Hughes, IBM, Infosys, Intel, Linx, Locaweb, Microsoft, Oracle, Promon Logicalis, Resource, SAP, Scopus, Spread, Stefanini, T-Systems, Tata, Tech Mahindra, Tivit, Totvs, Unisys.

São associados institucionais da Brasscom: B2B Magazine, CDI - Comitê para a Democratização da Informática, Centro de Tecnologia da Informação Renato Archer, C.E.S.A.R, Inatel – Instituto Nacional de Telecomunicações, USP – Universidade de São Paulo, UNESP – Universidade Estadual Paulista, UNICAMP - Universidade Estadual de Campinas, UFPE – Universidade Federal de Pernambuco.

Contribuições à consulta pública do Ministério da Justiça sobre o Anteprojeto de lei de Proteção de Dados Pessoais

São Paulo, 05 de julho de 2015

Introdução

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, entidade que congrega seleto grupo de empresas fornecedoras de software, soluções e serviços de TIC e que tem como missão trabalhar em prol do desenvolvimento do setor, disseminando seu alcance e potencializando seus efeitos sobre a economia e o bem-estar social, congratula o Ministério da Justiça pela inciativa da chamada de contribuições para o Anteprojeto de Lei sobre Proteção de Dados Pessoais.

É inquestionável o importante papel que a Internet tem na sociedade atual, tanto como viabilizadora de inclusão social quanto indutora de inovação e avanço tecnológico. Com efeito, a Lei 12.965 em 23 de abril de 2014 representa um importante avanço no tocante aos princípios que norteiam o papel da Internet no Brasil e ao regramento das relações jurídicas e responsabilidades entre os diversos atores sociais envolvidos. Perfilamo-nos com a sociedade brasileira ao festejar marco legal de tamanha envergadura, fazendo coro com os mais variados atores nacionais e internacionais.

Sem embargo de futuras e mais densas contribuições, a Brasscom serve-se desta oportunidade para deitar luz sobre alguns aspectos críticos que, entendemos, demandam atenta consideração por parte deste insigne Ministério.

Alterações Propostas e Respectivas Justificativas

O documento apresenta propostas de alteração de certos artigos, que são acompanhadas de justificativas com redação sumária. Algumas circunstâncias aludidas neste documento, referentes à dinâmica dos negócios no mundo digital demandariam textos substantivamente mais extensos para se tornarem cognoscíveis. No intuito de melhor fundamentar as proposições manifestadas neste documento, a Brasscom se coloca à disposição para esclarecimentos adicionais ou mais detalhados, que poderão incluir até mesmo certas demonstrações de situações de navegação por diferentes portais da Internet.

Na dicção dos dispositivos legais transcritos do Anteprojeto de lei de Proteção de Dados Pessoais objeto desta consulta pública adota-se a seguinte metodologia:

(i) ~~Fragmento de texto taxado~~ significa que propõe-se que o referido fragmento de texto seja eliminado do Anteprojeto de lei;

(ii) Fragmento de texto sublinhado significa que propõe-se que o referido fragmento de texto seja adicionado ao Anteprojeto de lei.

Capítulo I – Disposições Preliminares

[Art. 2]

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, exceto quando ocorrer o mero trânsito de dados no País, sem qualquer outra operação de tratamento, ou no caso de indivíduos temporariamente no país;

II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional exclusivamente para fins de oferta do produto e/ou serviço;

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

III - pertencentes a pessoas naturais não residentes no País;
IV - que sejam considerados dados anônimos ou de conhecimento público; ou
V– realizados por pessoa jurídica de direito público ou privado no âmbito das relações trabalhistas ou no cumprimento de dever legal.
VI– realizado nos serviços entre dispositivos M2M (máquina a máquina).

Justificativa

O processamento, armazenamento e tratamento das informações são realizados muitas vezes com envolvimento de múltiplas jurisdições. A redação original do anteprojeto de Lei impõe aos controladores e proprietários das informações ou dados (inclusive de outras nacionalidades e residentes fora do país) a sujeição a diferentes jurisdições, dependendo de onde os seus dados estiverem em um determinado momento.

Se as empresas tomarem suas decisões sobre os lugares nos quais os seus dados serão armazenados, tendo apenas como base considerações jurídicas, em desconsideração aos requisitos técnicos, poderíamos comprometer a sua capacidade de apresentar produtos adequados, de maneira rápida e eficaz aos seus clientes.

Se a legislação brasileira for aplicável aos dados coletados no Brasil, independentemente da residência e nacionalidade do sujeito proprietário dos dados, isso certamente gerará distorção no posicionamento do Brasil frente às demais jurisdições. A Lei brasileira rege os dados processados no país, os 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, ocasionando insegurança jurídica, devido a existência de jurisdições

múltiplas, que poderá ocasionar em um possível conflito de Leis, com o potencial de prejudicar o setor de TIC no Brasil, por exemplo, um controlador dos EUA pode optar por um processador de outro país, se dados dos EUA passarem a estar sujeitos à Lei, só porque o processador está baseado no Brasil. Nesse sentido, propõe-se que o escopo da Lei fique limitado aos dados coletados no Brasil, para evitar qualquer conflito de Leis quando dados oriundos do exterior forem processados no Brasil.

Adicionalmente sugere-se exclusões específicas, afastando a aplicação da Lei, no que se relaciona a cumprimento de dever legal e ainda a dados relacionados à relação de emprego. Nota-se, que cada 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.

Sugere-se ainda a exclusão das utilizações dos dados relativos a Internet das Coisas do âmbito do anteprojeto de Lei. A discussão envolvendo a Internet das Coisas ("IoT") é certamente embrionária. Muito se discute[1] a respeito dos princípios que podem ser adotados para regulamentar esse tipo de atividade, tendo em vista que, dada a sua natureza, certos tipos de controle inviabilizariam suas funcionalidades e desenvolvimento.

O conceito de Internet das Coisas abrange diversas funcionalidades atribuídas aos objetos do cotidiano que, conectados à Internet desempenham diversas outras funcionalidades. Podemos citar dispositivos para automóveis, residências e para uso pessoal, por exemplo que controlam o seu nível de sono e de exercícios diários, aparelhos que ajudam no acompanhamento médico, como o monitoramento para pessoas portadoras de diabetes. A gama de possibilidades é infinita. A estimativa é de que até 2020 existam 50 bilhões de dispositivos conectados no mundo.[2]

Dessa forma, regras que visem, por exemplo, as limitações ao tratamento de dados a um mínimo possível poderiam afetar o desenvolvimento, tendo em vista que novas funcionalidades e benefícios podem ser descobertos após a coleta dos dados.

Consentimento prévio e expresso por sua vez seria impraticável em uma infinidade de dispositivos que estão disponíveis para o uso em automóveis e residências, que controlam desde a navegação até a hora em que as luzes poderão ser acesas automaticamente. Em um exemplo ainda mais explícito, nos casos de pacientes que utilizam tecnologia para o monitoramento de saúde certamente não seria possível que o consentimento prévio e expresso fosse aplicado a cada coleta e tratamento de informações[3].

1 Em novembro de 2013 o FTC organizou nos Estados Unidos um debate público a respeito da privacidade e questão envolvendo a segurança diretamente relacionada, principalmente no que diz respeito ao desenvolvimento tecnológico.
2 http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
3 https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things

A regulamentação pode retardar o desenvolvimento dessas tecnologias, o que é indesejável. Sendo assim, se propõe que os dispositivos caracterizados como Internet das Coisas não estejam abarcados por essa Lei de proteção de dados.

[Art. 4-A] DO ÓRGÃO FISCALIZADOR

> **Art. 4-A° Fica constituída a Autoridade Nacional de Proteção de Dados Pessoais, entidade integrante da Administração Pública Federal indireta, com a função de órgão fiscalizador exclusivo das questões atinentes ao tratamento de dados pessoais, com sede no Distrito Federal.**
>
> **Parágrafo 1° A Autoridade atuará de forma independente, assegurando-se lhe, nos termos desta Lei, as prerrogativas necessárias ao exercício adequado de sua competência.**
>
> **Parágrafo 2° Caberá ao Poder Executivo instalar a Autoridade Nacional de Proteção de Dados Pessoais, devendo o seu regulamento, aprovado por decreto do Presidente da República, fixar-lhe a estrutura organizacional.**
>
> **Parágrafo 3° À Autoridade tem por finalidade principal executar no Território Nacional, as normas de proteção de dados pessoais, adotando medidas necessárias para o atendimento do interesse público e para a melhor interpretação e aplicação das normas de proteção de dados pessoais no País, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade.**

Justificativa

Leis gerais são baseadas em princípios amplos, permitindo interpretações adaptadas as circunstâncias daquele momento. O marco legal da proteção de dados pessoais tem a difícil missão de equilibrar a constante inovação baseada em dados, com a proteção do cidadão contra potenciais riscos e danos, garantindo o desenvolvimento tecnológico com as garantias necessárias de maneira harmônica.

Em função dos constantes avanços tecnológicos, o papel do intérprete das Leis gerais de proteção de dados torna-se ainda mais crucial. A experiência internacional evidencia que diretrizes claras trazem segurança jurídica e asseguram que as inovações observem a necessária proteção dos direitos do cidadão, ao passo que interpretações imprecisas geram incertezas podendo dificultar ou mesmo inviabilizar atividades empresariais legítimas, sem a proteção efetiva ao cidadão contra potenciais danos.

O anteprojeto de Lei especifica que caberá a um "órgão competente" interpretar, fiscalizar e fazer cumpri a Lei. Entendemos ser essencial a definição de qual seria este órgão, sua estrutura ou composição e suas atribuições essências.

Internacionalmente, quase todos os países que promulgaram Leis gerais de proteção de dados pessoais criaram conjuntamente um órgão nacional específico, independente e exclusivo, com a competência de interpretar, fiscalizar e fazer cumprir a Lei, normalmente denominado de "autoridade de proteção de dados" e referido pela sigla DPA ("*data protection authority*"). Entre as principais vantagens de um modelo de autoridade federal independente para a proteção de dados pessoais está a consistência das interpretações, a especialização técnico-

jurídica sobre o tema, a certeza regulatória e a independência necessária para atuar de modo eficaz e sopesar todos os direitos e interesses em jogo.

Entendemos que a designação de uma autoridade federal independente para a proteção de dados pessoais também é o modelo mais adequado para o Brasil, previsto, desde já, no anteprojeto de Lei. É fundamental que a interpretação e a sua fiscalização ocorram de forma harmoniosa e uniforme diante da amplitude das relações jurídicas que decorrem do uso da Internet no Brasil. Esse entendimento ocorre por se tratar de matéria de competência nacional, atendendo o que dispõe a Constituição Federal, que atribui à União a competência para legislar sobre normas gerais de natureza de Direito Civil. Ademais, fica claro a necessidade de especialização técnica-jurídica sobre um tema novo, com acúmulo de funções e abrangência multidisciplinar, em confluência com Direitos Pessoais e Direitos Civis resvalando em Direito Econômico.

Por fim, ressalve-se, 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.

[Art. 5 - I]

Art. 5° 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;~~ que identifique ou permita, por meios razoáveis, a identificação da pessoa natural, excluídos dados anônimos;

Justificativa

O texto do anteprojeto de Lei adota um conceito amplo de dado pessoal, mencionando que é considerado dado pessoal o "dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos".

Tal como redigido, o conceito engloba dados que não identificam uma pessoa natural, mas que estão meramente "relacionados" a ela. Com isso, ficariam sujeitos à Lei praticamente todos os dados produzidos pela atividade humana, ainda que não possam ser razoavelmente utilizados para identificar esse titular.

Um conceito mais preciso é adotado pela legislação do Canadá, "dados sobre uma pessoa natural", e se mostrou mais adequado para equilibrar a proteção do titular com o livre fluxo de informações.

Nas discussões mais recentes sobre o tema no âmbito da regulação geral de proteção de dados na Comissão Europeia (GDPR), têm-se sugerido que o conceito de dados pessoais seja revisado para englobar somente dados que razoavelmente permitam a identificação de uma pessoa natural, excluindo-se do conceito todos os dados que não sejam efetivamente capazes de

identificar razoavelmente um indivíduo, bem como todos os dados que passarem por processos de anonimização.

[Art. 5 - II]

> II – tratamento: conjunto de ações ~~referentes~~ a partir da coleta, que envolvam o uso de dados pessoais, que inclui a ~~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, transferência, ~~extração~~ ou difusão;

Justificativa

Sugerimos a simplificação da definição de modo a evitar a utilização de palavras que sejam sinônimos ou que possuam conceitos distintos em outros contextos, implicando em sua falta de clareza nas interpretações e consequentemente aplicação inadequada da norma.

A título de exemplo, fazemos referência ao uso da expressão "interconexão" que é, por definição contida em legislação específica (Lei no. 9.472/97)[4], a ligação entre redes de telecomunicações funcionalmente compatíveis para viabilizar um serviço de telecomunicações, com todas as implicações legais e tributárias que tal qualificação implica.

[Art. 5 - III]

> III – dados sensíveis: dados pessoais que ~~revelem~~ consistam na origem social e étnica, ~~as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso ou político, dados referentes~~ ~~dados referentes à saúde ou à vida sexual, bem como dados genéticos;~~ à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas;

Justificativa

A Lei nº 12.414 que disciplina o cadastro positivo determina em seu art. 3, § 3º que informações sensíveis, são "consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

Portanto, sugerimos a adoção da mesma definição de dados sensíveis constante em legislação existente, por uma questão de técnica e harmonização legislativa[5].

[Art. 5 - IV]

---

4 LGT - Artigo 146, Parágrafo único. Interconexão é a ligação entre redes de telecomunicações funcionalmente compatíveis, de modo que os usuários de serviços de uma das redes possam comunicar-se com usuários de serviços de outra ou acessar serviços nela disponíveis.

5 Informação que considero relevante: a parte conceitual foi retirada de alguma diretiva Europeia, como pode ser visto no *workbook* que trata dos *Privacy and Safeharbour Frameworks*:
http://www.export.gov/safeharbor/eg_main_018238.asp.
Vide Diretiva Europeia: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L

IV - dados anônimos - dados ~~relativos~~ ~~a~~ sobre 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;

Justificativa

Apesar de conceituar dados anônimos, o anteprojeto de Lei não menciona a expressão em nenhum outro ponto do texto. Para maior clareza, seria imprescindível observar que a) o tratamento de dados anônimos está fora do âmbito de aplicação da Lei e, justamente por isso, b) o tratamento de dados anônimos pode ser efetuado sem quaisquer exigências ou formalidades.

Sugere-se, assim, a inclusão de inciso III ao parágrafo 2º do art. 2º, para esclarecer que a Lei não se aplica aos tratamentos de dados anônimos, que podem ser tratados sem quaisquer exigências específicas, bem como menção expressa no art. 5º, inciso I, de que dados anônimos não são considerados dados pessoais, como mencionado anteriormente.

Além disso, sugerimos que a redação do artigo faça menção apenas à possibilidade de identificação por parte do responsável pelo tratamento, excluindo-se o complemento "nem por qualquer outra pessoa". Isso porque o responsável desconhece que outros meios podem ser empregados por terceiros ("outras pessoas") em tentativas de re-identificação de dados anônimos.

[Art. 5 - VII]

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

Justificativa

O conceito de consentimento é matéria que não goza de unanimidade entre as diversas jurisdições nacionais que se debruçaram sobre o tema. É útil, neste sentido, considerar a comparação entre o conceito incorporado no Anteprojeto de lei e seus congêneres a partir de outras fontes de direito internacionais. O art. 7º da Diretiva Europeia 95/46/CE menciona apenas "consentimento" de forma genérica, o que tem sido entendido na Europa como equivalente ao consentimento inequívoco, que pode ser obtido tanto de modo expresso quando inferido pelas circunstâncias e pelo contexto do tratamento dos dados.

O direito europeu reserva o consentimento expresso como regra geral apenas para as hipóteses de tratamento de dados considerados sensíveis, como se observa do art. 8º da Diretiva Europeia 95/46/CE.

A adoção de um conceito de consentimento inequívoco, em oposição a expresso, viabiliza o tratamento de dados no ambiente online, permite a contínua inovação baseada em dados e assegura um nível de proteção adequado ao titular sem gerar ônus excessivos para os responsáveis pelo tratamento de dados.

Ademais, do ponto de vista do titular dos dados, a exigência de obtenção de consentimento expresso para toda e qualquer atividade de tratamento de dados gera um fenômeno conhecido como "fadiga de consentimento", em que o titular passa a concordar com

todo e qualquer pedido de consentimento, ficando paradoxalmente menos protegido por não prestar atenção às hipóteses de tratamento que envolvem riscos maiores e que mereceriam maior cautela por parte do titular.

Sugere-se, portanto, a alteração do conceito de consentimento no anteprojeto de Lei, tanto no art. 5º, quanto no art. 7º, para que seja mencionado que consentimento é a manifestação "livre, inequívoca e informada do titular", bem como que dados pessoais somente podem ser objeto de tratamento "após o consentimento livre, inequívoco e informado do titular".

[Art. 5 - XI]

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

Justificativa

Sugerimos a exclusão da definição, para evitar a utilização de palavra que possui conceito distinto no contexto de telecomunicações, podendo levar a equívocos na aplicação da Lei.

Interconexão é uma expressão específica, com definição contida em legislação específica (Lei no. 9.472/97)[6], 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.

[Art. 5 - XII]

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

Justificativa

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

[Art. 5 - XIV]

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

Justificativa

Sugerimos que o conceito de dissociação de dados seja substituído por anonimização de dados, para garantir melhor harmonia nos conceitos trazidos pelo novo ordenamento legal.

6 LGT - Artigo 146, Parágrafo único. Interconexão é a ligação entre redes de telecomunicações funcionalmente compatíveis, de modo que os usuários de serviços de uma das redes possam comunicar-se com usuários de serviços de outra ou acessar serviços nela disponíveis.

A anonimização dos dados pessoais deverá ser considerada quando a reassociação de um dado pessoal ao seu titular não for simples ou razoável de ser feita pela parte que estiver fazendo o tratamento dos dados.

[Art. 5 - XV]

> XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de ~~qualquer~~ determinadas operações de tratamento;

Justificativa

Sugerimos que o bloqueio se restrinja a atividades específicas de tratamento, e não a toda e qualquer atividade de tratamento. Não são todas as atividades que podem ser suspensas em caráter temporário. 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.

[Art. 5 - XVI]

> XVI: cancelamento: eliminação, anonimização de dados ou do conjunto de dados armazenados em banco de dados, ~~seja qual for o procedimento empregado~~ sob controle do responsável, e não se estende aos dados porventura replicados em outros locais sob controle de outras entidades;

Justificativa

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.

[Art. 5 - XVII]

> XVII - uso compartilhado de dados: a comunicação, ~~a difusão~~, a transferência internacional de dados 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 delegado por esses entes público;

Justificativa

Sugerimos a exclusão dos termos "difusão" e "interconexão" do conceito de uso compartilhado de dados, em consonância com a consideração específica apresentada nos incisos XI e XII para a sugestão de exclusão desses termos.

[Art. 6 - I]

> 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~~ devidamente informadas ao titular;

Justificativa

Sugere-se a alteração de redação relativa ao princípio da finalidade, substituindo-se as expressões "específicas, explícitas e conhecidas" por "devidamente informadas", tendo em vista que a finalidade pode surgir em meio ao processamento de dados, viabilizando também usos inovadores dos dados.

[Art. 6 - III]

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

Justificativa

Sugere-se a substituição da palavra "mínimo" por " ao que for razoavelmente", tendo em vista que em diversos cenários, e para o benefício do próprio titular dos dados, o responsável limita o tratamento dos dados para um pouco além do mínimo, ou mesmo, pela impossibilidade de definição do que pode ser considerado "mínimo" para tal finalidade. Naturalmente, isso varia conforme o caso.

[Art. 6 - V]

V – princípio da qualidade dos dados, pelo qual deve ser garantida ~~a exatidão, a clareza e a atualização dos dados de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento~~ a integridade dos dados tais como fornecidos, para cumprir os seus respectivos efeitos de tratamento legalmente autorizado;

Justificativa

As empresas não devem ser responsabilizadas pela veracidade ou pela atualização dos dados coletados de terceiros. Hipóteses de responsabilidade devem ser restritas à integridade dos dados, ou seja, a guarda e a disponibilização dos dados tais como foram fornecidos.

[Art. 6 - IX]

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

Justificativa

A expressão "discriminação" tem diversos sentidos, inclusive o de selecionar dados específicos em bancos de dados. Assim, a discriminação que deve ser vedada é exclusivamente a ilícita. Todos os demais cenários em que há análise de dados para definição de perfis, análise de riscos e similares são legítimos e devem permanecer.

Capítulo II – Requisitos para o Tratamento de Dados Pessoais

Sessão I – Consentimento

[Art. 7]

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 quando tal fato decorrer da natureza própria do negócio jurídico ou 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~~ qualquer meio, cabendo ao responsável pelo tratamento dos dados pessoais a prova do consentimento ou por qualquer meio que o certifique.

§4º Quando necessário, o consentimento expresso 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.~~

~~§8o Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.~~

§9º Sem prejuízo do disposto nos parágrafos antecedentes, o consentimento se presume quando atendidos os seguintes requisitos de forma cumulativa:

I - o titular agir de maneira inequívoca e compatível com a outorga do consentimento, respeitado o disposto no §2º deste Art. 7º; e

II - os usos e costumes relativos ao negócio jurídico realizado entre titular e responsável forem compatíveis com o consentimento e a finalidade, observado o disposto no § 3º deste Art. 7º.

Justificativa

Tendo em vista a sugestão de alteração do conceito de consentimento previsto no art. 5º, inciso VII, para "manifestação livre, inequívoca e informada do titular para o tratamento de seus dados pessoais", sugere-se que o caput do art. 7º mencione apenas o termo "consentimento", evitando redundância.

Há diversos serviços prestados online que somente podem ser fornecidos gratuitamente quando há tratamento de dados pessoais. Assim, sugere-se alteração da redação do primeiro parágrafo, de modo a prever essas hipóteses.

É extremamente importante observar que há múltiplas maneiras de obter e provar o consentimento, não sendo compatível com o estado atual da tecnologia a exigência de consentimento por escrito para cada ato praticado pelo titular de dados, notadamente em serviços online. Sugere-se, assim, a unificação do parágrafo 3º com o parágrafo 8º do anteprojeto de Lei, pois ambos dispõem sobre o ônus que o responsável pelo tratamento tem em relação à prova do consentimento.

Ante a alteração sugerida acima, somente haverá necessidade de que o consentimento seja fornecido de forma destacada em relação às demais cláusulas contratuais quando sua manifestação de forma expressa for obrigatória.

Sugerimos a supressão do parágrafo 5º, pois com a evolução tecnológica a determinação prévia de todas as finalidades de tratamento de dados mostra-se difícil, notadamente em aplicações de big data, voltadas a extrair uma quantidade maciça de informações por meio da análise de bases de dados. Além disso, a utilização da expressão "autorizações genéricas" gera insegurança jurídica, por não se saber o seu efetivo significado

A possibilidade de revogação do consentimento a qualquer momento, sem ônus para o titular, gera grande insegurança jurídica, notadamente em serviços e conteúdo online gratuitos, cujo fornecimento depende do tratamento contínuo de dados pessoais. Assim, sugere-se igualmente a supressão do parágrafo 6º.

De forma a assegurar que o consentimento permaneça relevante e protetivo dos direitos do titular e, ao mesmo tempo, possa ser obtido em contextos dinâmicos e de modo compatível com o ordenamento jurídico brasileiro, é necessário que a Lei preveja hipóteses nesse sentido. Sugere-se, assim, a inclusão de um parágrafo ao art. 7º, relativo à possibilidade de presunção do consentimento.

[Art. 10]

Art. 10º No momento do fornecimento do consentimento, o titular será informado ~~de forma clara~~, ~~adequada e ostensiva~~ sobre os seguintes elementos:

I – finalidades ~~específica~~ do tratamento;

Justificativa

O fornecimento do consentimento pode ser informado de múltiplas formas. A referência à expressão "de forma clara, adequada e ostensiva" pode gerar insegurança jurídica. Sugere-se a alteração nos termos propostos na redação do artigo acima.

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".

O titular tem o direito de acessar, retificar ou revogar o consentimento em relação aos seus dados pessoais, e não a quaisquer dados. Sugere-se, assim, a inclusão da palavra "pessoais" inciso VII, alínea "b".

[Art. 11]

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:

VIII - legitimo interesse do responsável;
IX -realizado nos serviços entre dispositivos M2M (máquina a máquina).

Justificativa

O texto atual do anteprojeto de Lei dispõe em seu artigo 7º que, como regra geral, dados pessoais somente podem ser objeto de tratamento "após o consentimento livre, expresso, específico e informado do titular". Algumas exceções a essa regra geral são previstas no art. 11[7].

Na Diretiva Europeia, o consentimento do titular é apenas uma das modalidades que autorizam o tratamento de dados pessoais, não tendo o mesmo caráter de regra geral ora proposta, como se observa do artigo 7º da Diretiva Europeia 95/46/CE[8].

Uma das principais modalidades de tratamento de dados pessoais no sistema europeu é a existência de um interesse legítimo por parte do responsável. De acordo com essa modalidade, dados podem ser regularmente tratados, sem a necessidade de obtenção de consentimento, sempre que o responsável tiver interesse legítimo em tal tratamento, fazendo um balanceamento com os interesses, direitos e liberdades fundamentais do titular dos dados.

Ao interpretar esse dispositivo da Diretiva Europeia, o grupo de autoridades de proteção de dados da Europa, conhecido como "*Article 29 Working Party*", afirmou que essa modalidade de tratamento de dados estipula que o responsável faça um balanceamento ("*balancing test*"), entre seus interesses legítimos no tratamento dos dados e os interesses e direitos fundamentais do titular dos dados. O resultado desse balanceamento determina se os dados podem ou não serem legalmente tratados sem o consentimento do titular.

O *Article 29 Working Party* ressalta que esse balanceamento assegura aos responsáveis a flexibilidade necessária para efetuar o tratamento de dados nos casos em que não haveria impactos indevidos sobre o indivíduo em decorrência desse tratamento de dados. Por exemplo, o *Article 29 Working Party* considera que algumas atividades de marketing seriam permitidas, considerando esse balanceamento.

7 As exceções à necessidade de consentimento atualmente previstas no anteprojeto de Lei são:
a) dados de acesso público irrestrito; b) 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.
8 Conforme Diretiva Europeia 95/46/CE

A importância do interesse legítimo fica ainda mais evidenciada quando se constata que o conceito tradicional de consentimento não é adequado para lidar com o tratamento de dados em larga escala ("*big data*") nem com o cenário de novos dispositivos conectados (Internet das coisas). A inclusão da hipótese de interesse legítimo no anteprojeto de Lei brasileiro traria a segurança jurídica necessária para que o tratamento de dados pudesse ser efetuado de modo seguro e lícito pelos responsáveis, sem onerar os titulares com a necessidade de manifestação de seu consentimento a cada instante.

Nesse contexto, sugere-se a introdução, entre as exceções ao consentimento previstas no art. 11 do anteprojeto de Lei, do interesse legítimo do responsável como hipótese expressa de autorização para tratamento de dados pessoais, por meio da inclusão de um inciso adicional (VIII-legitimo interesse do responsável).

Por fim, caso a proposta de M2M (máquina a máquina) do escopo da Lei não seja acolhida, conforme recomendado no texto do parágrafo 2º do art.2 do anteprojeto de Lei, sugerimos que tal comunicação fique dispensada do consentimento nos moldes do art.11.

A discussão envolvendo a Internet das Coisas ("IoT") é certamente embrionária. Muito se discute[9] a respeito dos princípios que podem ser adotados para regulamentar esse tipo de atividade, tendo em vista que, dada a sua natureza, certos tipos de controle inviabilizariam suas funcionalidades e desenvolvimento.

O conceito de Internet das Coisas abrange diversas funcionalidades atribuídas aos objetos do cotidiano que, conectados à Internet possam desempenhas diversas outras funcionalidades. Podemos citar dispositivos para automóveis, residências, para uso pessoal e que controlam o seu nível de sono e de exercícios diários, aparelhos que ajudam no acompanhamento médico, como o monitoramento para pessoas portadoras de diabetes. A gama de possibilidades é infinita. A estimativa é de que até 2020 existam 50 bilhões de dispositivos conectados no mundo.[10]

Dessa forma, regras que visem, por exemplo, as limitações ao tratamento de dados ou o consentimento expresso para cada utilização poderão inibir ou inviabilizar o desenvolvimento de Internet das Coisas no país. Consentimento prévio e expresso seria impraticável em uma infinidade de dispositivos que estão disponíveis para o uso em automóveis e residências, que controlam desde a navegação até a hora em que as luzes poderão ser acesas automaticamente. Em um exemplo ainda mais explícito, nos casos de pacientes que utilizam tecnologia para o monitoramento de saúde certamente não seria possível que o consentimento prévio e expresso fosse aplicado a cada coleta e tratamento de informações[11].

A regulamentação nesse momento pode retardar o desenvolvimento dessas tecnologias em um período de crise financeira, quando elas poderiam ser mais necessárias. Sendo assim, se propõe que os dispositivos caracterizados como Internet das Coisas não estejam abarcados por essa Lei de proteção de dados.

---

9 Em novembro de 2013 o FTC organizou nos Estados Unidos um debate público a respeito da privacidade e questão envolvendo a segurança diretamente relacionada, principalmente no que diz respeito ao desenvolvimento tecnológico.
10 http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
11 https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things

Sessão II – Dados Pessoais Sensíveis

[Art. 12]

Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:

I - com fornecimento de consentimento ~~especial~~ expresso pelo titular:

~~§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.~~

Justificativa

Sugerimos que o consentimento para o uso de dados pessoais sensíveis seja permitido mediante o consentimento livre, expresso e informado do titular, e não mediante o consentimento especial do titular, sob pena de, em alguns casos específicos, como por exemplo a navegação de usuários por sítios na Internet ficar completamente prejudicada caso para cada *"click*" haja a necessidade de um novo consentimento para a utilização dos seus dados

No que tange ao parágrafo 2º do art.12, sugerimos a sua completa exclusão, pois na prática, tal artigo representa indevida ingerência na iniciativa privada e em modelos de negócios estabelecidos. Tome-se por base, por exemplo, as entidades cujo negócio central é a realização de análise de crédito dos consumidores. A base central de uma atividade como essa é, justamente, a utilização de dados sensíveis para estabelecer o perfil de crédito de um determinado consumidor, o que poderá, conforme o caso concreto, ser benéfico ou prejudicial, dependendo exclusivamente do consumidor em questão.

[Art. 13]

Art. 13. Órgão competente ~~poderá estabelecer medidas adicionais~~ fiscalizará as condições 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.~~

Justificativa

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 estipulados em Lei. Desse modo, sugerimos a substituição do texto proposto no caput do art.13 para que fique claro que caberá ao órgão competente a fiscalização das condições de segurança e não a adoção de novas medidas.

No que tange a proposta de texto para o parágrafo 1º do art. 13, 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. Desse modo, sugere-se a exclusão do parágrafo na forma como proposto.

Sessão III – Término do tratamento
[Art. 14]

Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

~~II - fim do período de tratamento;~~

III - comunicação do titular, quando houver razões preponderantes e legítimas para a solicitação do término do tratamento;

IV - determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar, desde que não haja outro remédio mais adequado para a sanção.

~~Parágrafo único - Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.~~

Justificativa

Para cumprir a finalidade de processamento de dados é necessário um período razoável, de acordo com a operação em questão, conforme modelo adotado pela Diretiva Europeia 95/46/EC, art. 7(f). O disposto no inciso II do art. 14 " fim do período de tratamento", da forma como proposto neste anteprojeto de Lei, compromete tecnicamente a liberdade dos modelos de negócios, e em especial a inovação em setores específicos, tal como o segmento de serviços online.

Para que se dê o término do tratamento de dados pessoais por comunicação do titular, não basta a comunicação apenas. É necessário ainda que se demonstre razões preponderantes e legítimas para justificar o término do processamento de modo que tal solicitação não seja utilizada de maneira indiscriminada pelo titular, evitando-se abuso desse direito por parte dos usuários dos serviços, conforme estabelecido na Diretiva Europeia 95/46/EC, art. 14. Embora declaradamente inspirado no arcabouço europeu de proteção de dados pessoais, o anteprojeto de Lei distancia-se do direito europeu, portanto sugere-se a alteração do inciso III do art. 14 para se ajustar a esses critérios.

Com relação ao parágrafo único do art. 14, a possibilidade do órgão competente poder solicitar o término do tratamento dos dados em decorrência de violação de dispositivo legal ou regulamentar, gera preocupação em virtude da possível limitação ao direito dos usuários que tal mandamento amplo pode gerar. Dessa forma, sugere-se a exclusão do dispositivo, ou caso se julgue mais apropriado, a sua qualificação no sentido de que o término do tratamento por determinação do regulador ocorra somente nos casos em que outra medida corretiva, dentre aqueles já elencadas no anteprojeto de Lei se mostre inadequada para a repressão da infração. Lembrando que a sanção deve, necessariamente, observar os princípios da razoabilidade, proporcionalidade e finalidade estabelecidos na Lei de Processo Administrativo Federal.

O texto do anteprojeto de Lei visa proteger e prestigiar os direitos e escolhas dos titulares de dados, que consentem que seus dados sejam usados e armazenados para a oferta de melhores

serviços e informações em seu próprio benefício. Por exemplo, os titulares podem optar por armazenar suas fotos em um serviço online com o objetivo de mantê-las num ambiente organizado e seguro, a decisão de armazenar estes dados por um período máximo, como disposto no parágrafo único do art.14 poderia gerar descontentamento por parte do usuário, ao descobrir que suas fotos devem ser apagadas por uma decisão do órgão competente de que o período máximo de armazenamento dessas fotos é de dois anos, com base na atual redação do parágrafo único do art. 14. De maneira geral, o anteprojeto de Lei deveria adotar mecanismos que permitam aos titulares o exercício pleno dos direitos com relação aos seus dados, permitindo escolhas informadas quanto ao uso e o compartilhamento dos seus dados pessoais.

Por tal razão, sugere-se a exclusão do parágrafo único do art.14.

[Art. 15]

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

IV – quando forem processados de tal forma que não se tratem mais de dados pessoais;

V—quando o titular assim consentir ou expressamente requerer.

Justificativa

Dentre as hipóteses de não cancelamento de dados após o seu processamento previstas nos incisos do art. 15, sugerimos incluir as seguintes: (a) dados anonimizados, ou seja, dados que tenham sido processados de modo que não possam ser considerados "dados pessoais"; (b) dados cujo processamento for expressamente requerido pelo titular; e (c) dados cujo processamento se der de acordo com o consentimento do titular. Estamos apenas começando a compreender o potencial dos diversos benefícios decorrentes do uso inovador dos dados pessoais em campos como a ciência, a medicina e as políticas públicas. 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 dados anonimizados ou baseado na escolha ou consentimento informado do titular.

Além disso, sugere-se a harmonização do art. 15 com o disposto no art. 7º, inciso X, do Marco Civil da Internet[12], conforme o qual o usuário tem direito à "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

No que diz respeito ao Parágrafo único do art. 15, cumpre ressaltar que o poder conferido ao órgão competente necessita ser harmonizado com o próprio direito à privacidade dos usuários, e os princípios da finalidade e razoabilidade da norma, sob pena de gerar grande insegurança jurídica e violação da privacidade do usuário decorrente de eventual ordem de manutenção de dados por período não razoável.

12 Conforme Lei 12.965, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
X - Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Capítulo III – Direitos do Titular

[Art. 17]

Art. 17. O titular dos dados pessoais tem direito a obter, com base na razoabilidade e disponibilidade de recursos:

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

IV – dissociação, bloqueio ou cancelamento de dados ~~desnecessários, excessivos ou~~ 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.

§ 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 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.

§ 3º Em caso de impossibilidade de adoção ~~imediata~~ da providência de que trata o §2º, o responsável enviará ao titular, ~~em até sete dias~~ dentro de um prazo razoável a partir da data do recebimento da comunicação, resposta em que poderá:

III - justificar de outra forma a impossibilidade de atendimento do pedido.

§ 4º A providência de que trata o § 2º será realizada sem ônus desproporcional para o titular.

§ 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.

Justificativa

A Diretiva Europeia de Proteção de Dados reconhece os direitos relacionados no art. 17, a saber: (a) confirmação da existência de dados em tratamento; (b) acesso aos dados; (c) retificação de dados; e (d) dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em conformidade com a Lei.

Por outro lado, o exercício desses direitos é balanceado com parâmetros de razoabilidade e disponibilidade de recursos. É importante que tais parâmetros sejam incluídos na proposta legislativa brasileira, para que se reduza a margem de situações em que o exercício abusivo de direitos individuais acabe por prejudicar o interesse coletivo. Nesse sentido, o art. 12º da Diretiva

Europeia 95/46 CE, ao tratar do direito de acesso aos dados pelo titular, indica balizas relacionadas a periodicidade razoável e sem custos excessivos.

Com relação ao item IV do art. 17 do anteprojeto de Lei, é importante que um parágrafo ressalve, nesses casos, os princípios constitucionais da liberdade de expressão e de imprensa, bem como do acesso à informação. Nesse sentido, o titular dos dados não poderá alegar que os dados são desnecessários ou excessivos, cerceando a opinião ou a informação pública. Por isso, sugere-se a remoção dos termos "excessivos" e "desnecessários", por serem subjetivos, restando a hipótese dos dados tratados em desconformidade com a Lei.

Ainda no caso inciso IV do art.17, é importante que a proposta legislativa preserve a possibilidade do responsável pelo tratamento de dados de cancelar eventuais serviços prestados ao titular dos dados, caso a dissociação, cancelamento ou bloqueio afetem tal serviço operacional ou economicamente.

O parágrafo 1º do art. 17 do anteprojeto de Lei estabelece o direito do titular de oposição ao tratamento de seus dados, quando ocorrer sem consentimento, caso discorde das hipóteses de dispensa de consentimento que se aplicavam àquele caso particular. Do ponto de vista do direito brasileiro, o texto disposto no §1º endereça o chamado direito de petição, assegurado na Constituição Federal entre os direitos fundamentais (Artigo 5º, incisos XXXIV e LXXIII).

Vale notar que a Diretiva Europeia 95/46 determina que as legislações dos membros da União Europeia apliquem esse direito, no mínimo, em casos em que a dispensa de consentimento se der em razão de tratamento por autoridade pública, em defesa do interesse público e em casos de tratamento dos dados por força do legítimo interesse do responsável.

Conforme mencionado nos comentários ao art. 11 do anteprojeto de Lei, é essencial que a legislação proposta adote a dispensa de consentimento por legítimo interesse, nos termos previstos no ordenamento europeu, a fim de garantir o ambiente adequado à inovação e ao surgimento de ferramentas que beneficiem a sociedade.

Recomenda-se que a proposta legislativa indique que o pedido deve ser atendido ou respondido em prazo razoável, levando-se em conta a sua própria complexidade, bem como da operação necessária para satisfazê-lo.

No que diz respeito ao §5º do art.17, que estabelece a obrigação do responsável pelo tratamento de dados de informar, aos terceiros a quem os comunicou, sobre a correção, cancelamento, dissociação ou bloqueio dos dados, para que procedam da mesma forma. Nesse caso, é importante que se adote no anteprojeto de Lei a ressalva prevista no item (c) do art.12º da Diretiva Europeia, excluindo os casos em que "for comprovadamente impossível ou implicar um esforço desproporcional".

[Art. 18]

> Art. 18. ~~A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:~~ 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.

~~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 razoavelmente permita o exercício do direito de acesso.

~~§ 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 fornecidos as informações e os dados ao titular.~~

Justificativa

O art. 18 do anteprojeto de Lei refere-se à maneira pela qual o responsável pelo tratamento de dados deve fornecer as informações solicitadas pelo titular quanto à existência e acesso aos seus dados pessoais.

Consideramos indesejável, neste caso específico, que uma Lei geral determine prazos que se apliquem igualmente a todos aqueles sujeitos às obrigações, que podem ter características e circunstâncias diversas. Além disso, o prazo estipulado de sete dias, úteis ou corridos, parece ser um prazo excessivamente reduzido, como regra geral. Sugere-se, assim, a adoção do critério de razoabilidade para a definição de prazo para cumprimento.

Da mesma forma, 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. Por isso, mais uma vez, recorre-se ao modelo da Diretiva Europeia, que apenas prescreve a "comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados" (art.12º, a).

[Art. 19]

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 ~~inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade~~ relacionados à sua capacidade profissional, financeira, creditícia e de moradia.

§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada, ressalvado o direito do responsável ao segredo de negócio.

Justificativa

O art. 19 outorga aos titulares o direito de solicitar aos responsáveis pelo tratamento de dados pessoais, a revisão de decisões tomadas unicamente com base em tratamento automatizado.

Nos dias de hoje, em que o tratamento de dados é parte integrante de praticamente todas as atividades produtivas, a automatização é essencial, em razão do volume de dados tratados. Por essa razão, a Diretiva Europeia 95/46, com o objetivo de balancear o direito do titular por meio do princípio da razoabilidade e da adequação, limitou o exercício desse direito a "determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora e comportamento". Parece-nos acertado tal balizamento, para evitar excessos que comprometam a qualidade dos serviços e garantam o acesso à informação que seja efetivamente relevante.

É importante que o processo de revisão a que se refere o art.19 não comprometa o segredo do negócio, ao dar ao titular acesso as informações sigilosas, cuja confidencialidade é essencial ao objetivo do responsável pelo tratamento. Nesse sentido, o Superior Tribunal de Justiça já decidiu em favor da manutenção do sigilo, ao analisar a validade do "*Credit Score*" à luz do código de Defesa do Consumidor e da Lei do Cadastro Positivo (Lei nº 12.414/2011)[13]. Informações relacionadas à segurança de transações financeiras, por exemplo, perdem sua eficácia se os critérios utilizados para prevenção à fraude forem acessíveis a potenciais fraudadores.

[Art. 20]

~~Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.~~

Justificativa

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.

Por isso, sugere-se a remoção do art. 20 ou a limitação de seu alcance ao uso de dados obtidos em desconformidade com a Lei.

[Art. 21]

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.

13 Superior Tribunal de Justiça (STJ), Segunda Seção, Recursos Especiais (Rep) nº 1.457.199 e 1.419.697, em 12/11/2014.

Justificativa

A garantia de aplicação das normas destinadas à tutela de direitos individuais e coletivos, conforme prevista no art. 21 do anteprojeto de Lei, é importante para assegurá-la ao cidadão e à sociedade.

No entanto, caso a Lei venha a prever a instituição de um órgão competente federal, central, independente e autônomo, para regular a aplicação das normas referentes ao tratamento de dados pessoais (vide comentários específicos sobre a "autoridade competente" no art. 4A), é desejável que o exercício em juízo seja balizado por interpretações uniformes advindos de tal órgão, inclusive com o objetivo de reduzir a judicialização excessiva de controvérsias.

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.

Capítulo IV – Comunicação

[Art. 22]

> **Art. 22. Nos casos de comunicação de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, ~~com quem terá responsabilidade solidária pelos danos eventualmente causados~~ sendo cada um deles responsável pelos atos que praticar.**
>
> **~~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.~~**

Justificativa

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.

De acordo com a proposta do anteprojeto de Lei, qualquer processador terá que assumir papel ativo ao tomar certas decisões a respeito do processamento de dados, o que pode vir a resultar em desvios das instruções do controlador. Portanto, recomenda-se a divisão das áreas de responsabilidade de cada um desses agentes de acordo com as suas funções e atos efetivos.

Além disso, diversas empresas possuem contratos de longo prazo que dispõem sobre a divisão de responsabilidades entre cedente e cessionário de dados. A observância deste dispositivo, tal como redigido originalmente, comprometeria essas obrigações contratuais e potencialmente desestimularia contrações e operações dessa natureza, prejudicando o ambiente de negócios no Brasil.

O termo interconexão foi suprimido em razão da sugestão de exclusão da respectiva definição.

[Art. 23]

> **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.**

Justificativa

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.

Além disso, embora o anteprojeto de Lei determine que o consentimento é necessário para qualquer comunicação de dados pessoais entre pessoas de direito privado, esse requisito acarreta em dificuldades operacionais e consequentemente aumento de custos para as empresas que pertencem ao mesmo grupo econômico ou que utilizam um prestador de serviços como processador de dados, pois, nesses casos, obter consentimento expresso de indivíduos implicaria esforços indesejados e desnecessários, além de gerar uma experiência ruim conhecida como a "fadiga de consentimento" para os usuários dos serviços dependentes do processamento de tais dados. 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.

É importante lembrar, ainda, que há motivações sociais e econômicas legítimas em grande parte da comunicação de dados realizadas pelas empresas, como a prevenção de fraudes, a cibersegurança e a busca de aperfeiçoamento na prestação de serviços aos consumidores.

O termo interconexão foi suprimido em razão da sugestão de exclusão da respectiva definição.

[Art. 24]

> **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:**
>
> ~~**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.**~~

Justificativa

A comunicação de dados pessoais entre pessoas de direito público deve depender do consentimento livre e informado, mas não necessariamente expresso e específico dos titulares.

Sugere-se a supressão do parágrafo único e seus incisos, dada a dificuldade de fragmentação do negócio, do próprio objetivo central e ainda maior proteção à privacidade dos titulares de dados nesses casos.

O termo interconexão foi suprimido em razão da sugestão de exclusão da respectiva definição.

[Art. 26]

> 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~~ ressalvado, quando aplicável, o direito do responsável ao segredo de negócio.

Justificativa

Sugere-se que a redação seja adaptada de modo que a referência final sobre a possibilidade de emissão de recomendações complementares visando a garantir o cumprimento da Lei seja suprimida, tendo em vista que uma norma com dispositivo tão amplo poderá trazer insegurança jurídica e incerteza ao ambiente de negócios.

Sugere-se ainda que seja incluída referência ao estrito respeito ao direito de confidencialidade quanto a segredos empresariais no âmbito de tais solicitações por parte do órgão competente.

O termo interconexão foi suprimido em razão da sugestão de exclusão da respectiva definição.

[Art. 27]

> ~~Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.~~

Justificativa

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.

Capítulo V – Transferência Internacional de dados

[Art. 28]

> 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:

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;

VI - quando houver sido obtido consentimento do titular para a transferência;

VII - .quando a transferência for feita para entidade que tenha se comprometido a observar regras de proteção de dados consistentes com as obrigações previstas na lei brasileira.

Justificativa

Conforme as regras da APEC (*Asia Pacific Economic Cooperation*), é permitida a transferência internacional de dados em todas as situações específicas previstas nos arts. 28 e 30 (BCRs).

No caso do inciso III do art. 28 e do caput do art. 30, quando a empresa adota a cláusula padrão elaborada pelo órgão competente, não há necessidade de autorização prévia desse mesmo órgão.

Dentre as exceções previstas nos incisos do art. 28, sugerem se a inclusão : a) mais precisamente no inciso II, a hipótese em que a transferência for necessária à proteção da vida ou da incolumidade física do responsável ou de seus membros; (b) em complementação à lista de exceções, a hipótese em que for obtido o consentimento do titular para a transferência internacional dos seus dados; (c) e também em complementação à lista de exceções, a hipótese em que a transferência for feita para um entidade que tenha se comprometido a observar regras de proteção de dados consistentes com as obrigações previstas na lei brasileira.

De modo a evitar autorizações, caso a caso, e análises longas e custosas que podem atrasar demasiadamente uma série de negócios no setor de TIC, o órgão competente poderá: (a) estabelecer uma lista aberta de países que proporcionam nível adequado de proteção, nos moldes do que é feito pela Comissão Europeia; e (b) a possibilidade de que as próprias empresas sejam listadas pelo órgão competente em listas abertas de empresas que observam adequadamente as regras sobre proteção de dados.

Por fim, entendemos que a estrutura proposta para o art. 28, objetiva permitir que a transferência internacional de dados possa ocorrer, independentemente de consentimento do titular, para os países que proporcionem nível de proteção de dados pessoais comparáveis ao da Lei. Sendo esse esclarecimento essencial para a correta aplicação da Lei, sugere-se a adequação do texto proposto para clarificar tal mandamento.

Nessa mesma linha, em busca de uma melhor técnica legislativa e maior clareza na aplicação da Lei, sugere-se a inclusão de um inciso no art. 28 para permitir a transferência internacional de dados para países que não ofereçam o mesmo nível de proteção da Lei, desde que para tal caso haja um consentimento especial do titular.

[Art. 29]

~~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.~~

Justificativa

Tendo em vista a proposta de alteração do art. 28, de inclusão de um inciso específico, que determine como uma das hipóteses de exceção à regra da transferência internacional de dados sem o consentimento do titular, a situação de transferência dos dados para um país que não possua o mesmo nível de proteção, garantido pela Lei, desde que haja um consentimento especial do titular para tal transferência, sugere-se a exclusão do art. 29.

[Art. 30]

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.

§3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ~~ou realizar diligencias de verificação~~ quanto às operações de tratamento.

§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.

Justificativa

Sugere-se a inclusão de um parágrafo dispondo que o órgão competente precisa considerar a possível natureza global da operação de processamento, não vinculando 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.

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.

Com base no item 5.2[14] do *"Working Document: Transfers of personal data to third countries: Applying Article 26 of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", sugere a exclusão a referência no §3º do art. 30, à realização de "diligências de verificação quanto às operações de tratamento" por parte do órgão competente. O que se deve ser estimulado é a realização de auditorias internas ou supervisionadas por auditores independentes, que poderão enviar cópias dos documentos referentes a tais atividades ao órgão competente.

[Art. 31]

~~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.~~

Justificativa

Conforme se argumentou no art. 22, a cada um dos agentes devem ser atribuídos os deveres e responsabilidades respectivos aos seus próprios atos, o conceito de responsabilidade solidária nos casos de transferência internacional poderá acarretar uma responsabilidade indevida dos agentes envolvidos em uma operação de tratamento, e logo em insegurança jurídica, portanto sugere-se a exclusão do art. 31.

[Art. 32]

~~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.~~

Justificativa

A aplicação da Lei nacional se orienta pelo princípio da territorialidade, em regra, as Leis de origem doméstica de cada país se aplicam às relações atreladas ao seu território (e.g., Código Penal, art. 5º).

Dessa forma, recomendamos que a lei brasileira não exija o cumprimento das normas de outros países, a menos que por motivos legítimos e razoáveis. Sugere-se que este dispositivo, seja excluído do projeto de Lei proposto.

[Art. 33]

~~Art. 33. 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.~~

14 "5.2. Audits – The rules must provide for self-audits and/or external supervision by accredited auditors on a regular basis with direct reporting to the ultimate parent's board. Data Protection Authorities will receive a copy of these audits where updates to the rules are notified and upon request where necessary in the framework of the co-operation with the data protection authority."

Justificativa

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.

Capítulo VII – Responsabilidade dos Agentes

Seção I – Agentes do Tratamento e Ressarcimento de Danos

[Art. 35]

> **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.**
>
> **§ 2º O responsável ou o operador ~~podem deixar de ser~~ não serão responsabilizados se provarem que o fato que causou o dano não lhes é imputável.**

Justificativa

A determinação da responsabilidade dos agentes deve considerar, de forma inequívoca, a natureza do tratamento dos dados e a imputabilidade dos danos causados em sua decorrência. A título exemplificativo, há situações em que o potencial lesivo decorrente do tratamento pode não guardar qualquer relação de culpa ou dolo por parte dos agentes, como em casos de mero armazenamento remoto de dados.

Qualquer agente que estiver processando informações pessoais, deve estar sujeito a obrigação de confidencialidade em conformidade com a Lei, mas a responsabilidade civil conjunta, como mencionada no anteprojeto de Lei, pode não ser compatível com as funções reais das partes. Um controlador pode determinar as finalidades e os meios de processar informações pessoais. Por outro lado, um processador não possui a autoridade para atribuir a responsabilidade que um controlador possui. Ele apenas pode seguir as instruções do controlador. Essa distinção é importante porque o controlador (e não o processador) é quem deve ser o principal responsável pela conformidade com as respectivas obrigações de proteção de dados e por determinar os meios e controles para a proteção dos dados. Uma diferenciação sem deixar margem a dúvidas entre as funções, serve para estabelecer uma atribuição clara dos deveres e responsabilidades e ajuda a esclarecer casos complexos, nos quais os dados são processados por mais de uma entidade (por exemplo, terceirização de processamento). De acordo com o arrazoado do anteprojeto de Lei, o processador terá que assumir um papel ativo ao tomar certas decisões a respeito do processamento, o que poderia resultar em desvios das instruções do controlador. Esse critério acarreta um risco significativo de causar danos à comunidade de TIC no Brasil.

[Art. 38]

> **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.

Justificativa

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, portanto sugere-se que seja inserido no art.38 o complemento "observados os limites estabelecidos em Lei"

Seção II – Responsável e Operador

[Art. 39]

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.**~~

Justificativa

Recomenda a supressão do § 1º do Art.39, pois a responsabilidade solidária entre controlador (cessionário) e processador (cedente) de dados da forma como proposta no anteprojeto de Lei, acarretará em responsabilização indevida dos agentes envolvidos em uma 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.

Recomenda-se, que seja suprimido o § 2º do art.39, na medida em que facultam 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.

[Art. 40]

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**~~.

Justificativa

Recomenda-se, que seja suprimido o parágrafo único do art. 40, na medida em que facultam 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.

Seção IV – Segurança e Sigilo dos Dados

[ART 42]

> **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, ou qualquer forma de tratamento inadequado ou ilícito.**

Justificativa

Em relação às medidas de segurança técnica, a referência a "constantes atualizações" precisa ser mediada pela razoabilidade dos intervalos de que trata o artigo, conforme a natureza e porte das entidades envolvidas no processamento dos dados e pelo tipo e criticidade dos dados por ela manipulados.

Da maneira como disposto no anteprojeto de Lei poderá gerar insegurança sobre a periodicidade de tais atualizações. Entendemos que o parágrafo único resolve de maneira clara a questão, podendo a referência a constantes atualizações ser eliminada do artigo.

[ART 43]

> **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~~ de respeitar os limites do consentimento obtido no ato da informação dos dados pessoais, quando aplicável, mesmo após o seu término.**

Justificativa

No que se refere ao art. 43, quando trata do dever de sigilo, entendemos que a obrigação deve ser compatível com os termos de consentimento estabelecidos no ato da informação dos dados pessoais.

O dever de sigilo é em verdade um caso particular que se aplica a determinados tipos de dados e consentimento. Deste modo, sugerimos a redação proposta acima, não expandindo tal conceito a toda e qualquer hipótese de término de tratamento.

[ART 44]

Art. 44. O responsável deverá comunicar ~~imediatamente~~ 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.

§ 1º A comunicação deverá mencionar, no mínimo:

III - indicação das medidas de segurança utilizadas para a proteção dos dados, ~~inclusive procedimentos de encriptação~~;

§ 2º Para fins do caput do Art. 44, considera-se incidente de segurança o evento, que foge ao controle do responsável, em que ocorre efetiva transferência de dados pessoais a terceiro não autorizado, que potencialmente causa danos significativos aos titulares.

Justificativa

O anteprojeto de Lei não é claro ao determinar os incidentes de segurança que devem ser notificadas e que informações devem ser apresentadas, portanto recomenda-se que as notificações somente sejam obrigatórias nos casos de falhas que impliquem em danos significativos aos indivíduos e que nestes casos sejam apresentadas maiores orientações.

O prazo para as notificações pode variar de acordo com a proporção do incidente, tendo como base experiências anteriores em outros países, as notificações imediatas encontram algumas dificuldades, pois é necessário despender tempo e esforço para estabelecer a causa-raiz das falhas e corrigi-las adequadamente. As notificações somente são possíveis quando esses dois aspectos tiverem sido completamente resolvidos.

Entendemos que o conceito de medidas de segurança atualmente já inclui informações relacionadas a criptografia quando aplicável. No entanto, a redação do texto legal deve ser neutra do ponto de vista tecnológico, em vista das constantes mudanças de tecnologia ao longo do tempo, por isto sugere a supressão da referência expressa do procedimento de encriptação.

[ART 45]

Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:

§ 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.

Justificativa

O prazo para as notificações deve variar de acordo com a proporção do incidente, tendo como base experiências anteriores em outros países, as notificações imediatas encontram algumas dificuldades, pois é necessário despender tempo e esforço para estabelecer a causa-raiz das falhas e corrigi-las adequadamente. As notificações somente são possíveis quando esses dois aspectos tiverem sido completamente resolvidos.

[ART 47]

~~Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.~~

Justificativa

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, assim sugerimos a exclusão do Art. 47.

Seção V – Boas Praticas

[ART 49]

Art. 49. ~~O órgão competente estimulará a adoção de~~ os agentes econômicos poderão adotar padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais~~, incluindo o direito ao não rastreamento.~~

Justificativa

Tendo em vista a dinamicidade de certos mercados, em especial a indústria online, a permissão para que o órgão competente intervenha na elaboração e/ou adoção de padrões técnicos poderá vir a representar um engessamento no processo de inovação.

Desse modo, sugerimos que, deixe a cargo dos vários stakeholders a definição de quais padrões técnicos deverão ser adotados para facilitar a disposição dos titulares sobre seus dados pessoais.

É de responsabilidade da indústria a definição da estrutura tecnológica que lhe é possível administrar, implementar e custear livremente, atendendo a legislação de modo a não lhe causar prejuízo ou onerosidade, sempre com observância aos direitos dos titulares e consumidores, conforme estabelecido em legislação específica.

Capítulo VIII – Sanções Administrativas

[ART 50]

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 com limite a ser definido em Lei;

~~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.~~

§ 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.

~~**§ 4o O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.**~~

Justificativa

Embora um sistema de sanções para o descumprimento das normas seja absolutamente fundamental, acreditamos que por uma questão de segurança jurídica e previsibilidade dos negócios, é importante que a Lei traga certos parâmetros para sua aplicação.

É necessário considerar que a crescente utilização de normas abertas, que possibilitam o seu enquadramento de forma discricionária no caso concreto pelo agente administrativo, buscando atender as necessidades coletivas, também podem acarretar prejuízos aos administrados.

"A razoabilidade é um conceito jurídico indeterminado, elástico e variável no tempo e no espaço. Consiste em agir com bom senso, prudência, moderação, tomar atitudes adequadas e coerentes, levando-se em conta a relação de proporcionalidade entre os meios empregados e a finalidade a ser alcançada, bem como as circunstâncias que envolvem a pratica do ato"[15].

O princípio da razoabilidade ou da proporcionalidade - expressão mais comum, especialmente no Brasil, entre os constitucionalistas[16], é comum a todos os ramos do direito.

Dessa forma, permanecendo a margem para atuação do poder administrativo, em efetivar as determinações legais, recomenda-se a adoção de critérios que atendam equilibradamente a finalidade pública, no que também se insere não prejudicar o agente particular de maneira que lhe cause a inviabilidade do negócio.

Sugerimos a exclusão do parágrafo 4 em vista da nossa proposta de criação de uma autoridade única federal competente para interpretar e aplicar sanções relacionadas ao eventual descumprimento desta Lei.

Ainda em respeito ao princípio da proporcionalidade, sugerimos a exclusão dos incisos VII e VIII do artigo que ao proibirem de maneira total e coercitiva, por um prazo tão longo quanto dez anos, o tratamento de dados poderão levar ao desaparecimento de empresas que exerçam suas atividades no território nacional, bem como ao descumprimento de certas obrigações legais por empresas que estejam aqui presentes.

Veja-se, por exemplo, a situação de uma empresa que cometa uma infração nos termos da legislação ora proposta e fique proibida de rodar a sua própria folha de pagamento por um

15 RESENDE, Antonio José Calhau. O princípio da Razoabilidade dos Atos do Poder Público. Revista do Legislativo. Abril, 2009.
16 BARROS, Suzana de Toledo. O Princípio da proporcionalidade e o Controle de Constitucionalidade das Leis restritivas de Direitos Fundamentais. Brasília: Brasília Jurídica, 1996. pp. 24 e 69.

período de até 10 anos. Nessa linha, entendemos que as outras sanções já identificadas no art. 50 são suficientes para punir uma eventual infração da Lei, sem, contudo, prejudicar o funcionamento de uma empresa produtiva ao longo do tempo.

De modo a garantir a correta aplicação dos instrumentos sancionatórios previstos no art. 50, reiteremos a sugestão de que os valores arrecadados com as multas impostas nos termos desse artigo não façam parte do orçamento operacional do órgão competente, para que não se crie um incentivo a aplicação de sanções que sejam demasiadamente severas em face de eventuais infrações ao dispositivo da Lei.

CAPÍTULO IX - Disposições transitórias e finais

[Art. 51]

> ~~**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.**~~

Justificativa

Sugere-se que o art. 51 seja um parágrafo único do art. 52, devido à complexidade das obrigações estabelecidas nesse anteprojeto de Lei, sugere-se, que as normas de adequação progressiva sejam uma discricionariedade do órgão competente, propondo a alteração do texto "estabelecerá" por "poderá", conforme redação sugerida para o art.51.

[Art. 52]

> **Art. 52 - Esta Lei entrará em vigor no prazo de ~~120 (cento e vinte) dias~~ 2 (dois) anos contados data da sua publicação**
>
> **Parágrafo único. Órgão competente poderá estabelecer 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.**

Justificativa

Tendo em vista a complexidade das obrigações estabelecidas nesse anteprojeto de Lei, e os inúmeros ajustes técnicos que serão necessários em vários segmentos industriais para a sua efetiva implementação, incluindo dentre outras medidas a aquisição ou desenvolvimento de programas de computador específicos, sugerimos que a Lei entre em vigor somente após 2 (dois) anos a partir da data da sua promulgação.

Toma-se por referência a *vacatio legis* adotada pela União Europeia quando passou pela adoção de obrigações de proteção de dados muito similares àquela hora propostas.

Certos de que as contribuições representam importante etapa na regulamentação do anteprojeto de Lei sobre Proteção de Dados Pessoais, reiteramos nosso apoio à bem-vinda iniciativa do Ministério da Justiça.