Anteprojeto de Lei de Dados Pessoais – Fev.2015	Comentários e Sugestões da Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (ABDTIC)
CAPÍTULO I – DISPOSIÇÕES PRELIMINARES	
Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.	
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; ou II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.	Como os dados a que o art. 2º, I e II, se refere podem ter sido tratados apenas parcialmente em território nacional, sugerimos incluir que a lei será competente para os casos em que o tratamento ocorrer integral ou parcialmente em território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Esta Lei não se aplica aos tratamentos de dados:	
I – realizados por pessoa natural para fins exclusivamente pessoais; ou	Considerando que a "pessoa natural" poderia tratar os dados pessoais de outrém com fins dolosos, sugerimos substituir o inciso I pela seguinte redação: "*realizados sem dolo por pessoa natural para fins exclusivamente pessoais; ou*".
II – realizados para fins exclusivamente jornalísticos.	
§ 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado. Art. 3º As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.	No parágrafo 3º do art. 2º e parágrafo único do art. 3º, sugerimos inserir a previsão de que as entidades privadas que receberem dados de órgãos públicos serão obrigadas a apagarem tais dados assim que se conclua o tratamento ou fim específico a que se destinavam os dados, não havendo a possibilidade de manutenção destes pela entidade privada.
Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei. Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente. Art. 5º Para os fins desta Lei, considera-se:	
I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;	

II – tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;	Há verbos neste inciso que podem ser considerados sinônimos, como "*transmissão" e "distribuição",* e "*arquivamento" e armazenamento*", sendo possível a exclusão de um dos sinônimos. Outros termos utilizados podem ser confundidos com termos legais definidos em outras leis como é o caso de *interconexão* utilizada e definida na regulação de telefonia. Assim, sugerimos substituir "*interconexão*" por "*cruzamento*".
III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;	O termo "que revelem" dá margem a interpretações possivelmente errôneas. O ideal seria "dados pessoais consistentes em..."] A inclusão de convicções *filosóficas ou morais* é demasiadamente ampla e pode dar margem a interpretações errôneas. Sugerimos sua exclusão ou limitação.
IV – dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;	Para a segurança do titular, seria necessário estabelecer que dados anônimos devem permanecer como tal, não podendo ser objeto de tratamento para sua posterior identificação.
V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;	Os bancos de dados podem estar localizados no país ou fora dele. Assim sugerimos incluir "*localizado em um ou em vários locais, no país ou fora dele…"*
VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;	
VII – consentimento: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;	É necessário prever que o consentimento pode ser expresso e livre, mas também tácito quando o uso de determinado serviço precisar do fornecimento de determinados dados para que seja possível seu funcionamento. Também é necessário prever o formato padrão de consentimento através de check box em formulários. Diante disso, nossa sugestão de redação seria: " VII – consentimento: manifestação livre, expressa ou tácita inequívoca, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma ou mais finalidades determinadas. O consentimento tácito só ocorrerá nos casos em que o funcionamento precípuo e principal de determinado produto ou serviço pressupor o fornecimento de determinados dados pessoais."
VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável; X – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;	
XI – interconexão: transferência de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;	No inciso XI do art. 5º, sugerimos a retirada do termo "*interconexão*" e sua substituição por "*cruzamento*", uma vez que o termo "*interconexão*" já é utilizado na regulamentação de telefonia com outro significado. Ainda, a proposta de definição de interconexão foi redigida de forma muito ampla e vaga como se se estivesse tratando de uma mera transferência ou comunicação de dados, pelo que não é possível pela redação atual entender a diferença entre comunicação de dados e interconexão. Desta forma,sugerimos a seguinte redação *"Interconexão: tratamento de dados que consiste no relacionamento dos dados pessoais constantes de um ficheiro com os dados de um outro ficheiro ou ficheiros mantidos ou não pelo mesmo ou outro(s) responsável(is), ou mantidos pelo mesmo responsável com finalidade semelhante ou distinta."*
XII – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma; XIII – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;	

XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável; XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;	
XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;	No inciso XVI, o termo "*cancelamento*" pressupõe a ideia de término de determinado serviço. Para a definição proposta, o ideal seria o termo "*apagamento*" ou "*exclusão*".
XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e	No inciso XVII, sugerimos a substituição do termo "*interconexão*" por "*cruzamento*".
XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente. XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente. Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais: I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular; II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades almejadas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento; III – princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;	
IV – princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;	No inciso IV, sugerimos incluir que o acesso sempre será dado mediante requisição prévia e por escrito, de maneira eletrônica ou física, a critério do responsável.
V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento; VI – princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;	
VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;	Sugerimos especificar que a discriminação exposta deve ser "*não Ilícita*", tal como ocorre com o cadastro positivo.
VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e IX – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios. § 1º Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.	

§ 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.	
CAPÍTULO II – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS	
Seção I – Consentimento	
Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.	Já há menções de que o consentimento deve ser livre e expresso em sua definição. Sugere-se a retirada destes trechos do artigo.
§1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização. §2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.	
§3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.	Sugerimos a seguinte redação para este parágrafo: "*§3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique* ***posteriormente*** *."*
§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.	Tal destaque poderia ser feito mediante uso de *check box* como é o padrão atual de melhores práticas sobre este tema. Dessa forma, sugerimos a seguinte redação para este parágrafo: "*§4º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique posteriormente. O consentimento poderá ser fornecido mediante aceite e marcação de check box específico em formulários de dados* ."
§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.	Sugerimos a seguinte redação para este parágrafo: *"§5º O consentimento deverá se referir a finalidades determinadas e* ***descritas previamente à coleta ou tratamento de dados pessoais*** *, 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.	Como o consentimento só poderá ser revogado por escrito e mediante a confirmação de seu titular, sugerimos a seguinte redação para este parágrafo: "*§6º O consentimento pode ser revogado a qualquer momento, por escrito e mediante confirmação do titular, sem ônus adicional para este* ."
§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.	
§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.	As provas de consentimento podem ser apagadas após o término dos serviços ou solicitação de exclusão dos dados? Poderia ser aplicada analogia aos dados de conexão?
Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse. Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento. Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:	

I – finalidade específica do tratamento; II – forma e duração do tratamento; III – identificação do responsável; IV – informações de contato do responsável; V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita a: a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º; b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.	
§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.	O ideal é que a redação preveja que tais dados são anuláveis, não nulos, já que a interpretação sobre a forma de apresentação do pedido de consentimento dependeria de uma série de questões que deveriam ser melhor definidas.
Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:	Qual seria a definição de "*dados de acesso público*"? Se os dados pessoais tiverem sido disponibilizados em redes sociais pelos próprios titulares, eles serão considerados dados privados de acesso público? Eles estarão sujeitos à proteção estabelecida nessa lei? No art. 11 entendemos que deverá ser incluida uma outra exceção para o consentimento que é o tratamento de dados sempre que houver que "interesse legítimo", ou seja, casos em que o tratamento dos dados é essencial à execução do serviço para o qual o titular forneceu os dados. A propósito, este é um dos pressupostos do tratamento de dados previstos na Diretiva de Proteção de Dados da União Europeia. O interesse legítimo aqui indicado deverá ser: (a) um interesse legítimo do responsável ou de um terceiro a quem sejam fornecidos os dados (por exemplo, no caso de o titular deixar de pagar determinada prestação a um banco e este fornecer os seus dados pessoais a uma empresa de cobrança para obter o pagamento da dívida pelo titular dos dados, embora o titular não tenha consentido), (b) esta exceção do interesse legítimo deve respeitar os princípios de proteção de dados (princípio da qualidade dos dados e o princípio da necessidade e adequação, i.e., os dados devem estar atualizados, e apenas serem transmitidos quando essenciais à finalidade).
I – cumprimento de uma obrigação legal pelo responsável; II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública; III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º; IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; V – exercício regular de direitos em processo judicial ou administrativo; VI – proteção da vida ou da incolumidade física do titular ou de terceiro;	

VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.	
§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.	Ao invés de prever que o uso dos dados seria pelo menor tempo possível, o ideal seria definir o prazo máximo de sua utilização.
§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º. § 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.	
Seção II – Dados Pessoais Sensíveis	
Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:	
I – com fornecimento de consentimento especial pelo titular:	Qual seria a definição de "*consentimento especial* "?
a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para: a) cumprimento de uma obrigação legal pelo responsável; b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública; c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; d) exercício regular de direitos em processo judicial ou administrativo; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias. § 1º O disposto neste artigo aplica-se a qualquer tratamento capaz de revelar dados pessoais sensíveis.	
§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.	Qual seria a extensão da expressão "*em detrimento do titular*" ? Caso o tratamento dos dados pessoais prejudique ou possa prejudicar de alguma forma o titular, então estes dados não poderiam ser tratados? A redação do parágrafo está muito ampla e sujeita a más interpretações.
§ 3º Nos casos de aplicação do disposto nos itens 'a' e 'b' pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do §1o do art. 6o.	
Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.	Os dados pessoais sensíveis não podem ser entregues ao órgão de Governo sem anuência prévia ou ordem judicial que o preveja. O órgão de Governo deve apenas requisitar melhores medidas de proteção, sem contudo exigir a guarda e/ou administração de tais dados.
§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.	

§ 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.	
Seção III – Término do Tratamento	
Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade específica almejada; II - fim do período de tratamento;	
III – comunicação do titular; ou	Neste inciso III, ao invés de "comunicação do titular", não seria melhor a expressão "revogação do titular" como usado nos demais termos do APL?
IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.	
Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.	A interferência do Estado no direito do titular de dados de exercer o direito de requerer o tratamento de seus dados deve ser a exceção e não a regra. Por isso, o que o parágrafo único deveria estabelecer o seguinte: "*Órgão competente poderá estabelecer períodos máximos para o tratamento de dados pessoais, nos casos previstos em lei"*.
Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal pelo responsável; II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou	
III – cessão a terceiros, nos termos desta Lei.	Sugerimos a substituição do termo "*cessão*" por "*transferência"*, já que este é o único dispositivo em que consta a palavra "*cessão"*. Já a palavra "*transferência"* está nas definições de "*comunicação de dados"*, "*interconexão"*, "*difusão"* e "*transferência internacional de dados"*.
Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.	Neste parágrafo, há também uma inversão de valores. É o regulador que deve ser balizado pela Lei e não o contrário. É a Lei que deve estabelecer hipóteses de exceção ao direito de cancelamento de dados pessoais, cabendo ao regulador implementá-las.
CAPÍTULO III – DIREITOS DO TITULAR	
Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.	
Art. 17. O titular dos dados pessoais tem direito a obter:	Alguns dos direitos mencionados no art. 17 só podem ser adequadamente exercidos com a utilização de dados que possam autenticar a identidade do solicitante, sob pena de resultarem em fornecimento indevido de informações a terceiros não autorizados. É o caso, por exemplo, do acesso aos dados armazenados por prestadores. Além disso, certos procedimentos de tratamento de dados, como a dissociação, tornam impossível o exercício de alguns desses direitos. Por isso, sugerimos a inclusão de dispositivo para esclarecer que determinados direitos somente poderão ser exercidos mediante a identificação da pessoa natural.
I – confirmação da existência de tratamento de seus dados; II – acesso aos dados;	

III – correção de dados incompletos, inexatos ou desatualizados; e	A lei deve esclarecer que este dispositivo refere-se apenas aos dados pessoais *per se* e não à informação que o qualifica, para que não se dê margem a interpretação que restrinja, de alguma forma, a liberdade de expressão e de informação. Por isso, sugerimos a inclusão de um novo parágrafo no artigo 17, com a seguinte redação: *"§6º O disposto nos incisos III e IV refere-se exclusivamente aos dados per se e não confere ao titular o direito de requerer a modificação ou cancelamento:* *(i) de informações, opiniões e outras qualificações ou adjetivações lícitas associadas a seus dados pessoais, preservando-se o direito à liberdade de expressão e manifestação do pensamento de terceiros; e* *(ii) de informações, opiniões e outras qualificações ou adjetivações lícitas que eram atuais e exatas quando de sua publicação ou comunicação, preservando-se a história e o direito de acesso à informação e à história."*
IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.	Sugerimos a inclusão de um parágrafo 6º, conforme comentário anterior em relação ao inciso III.
§1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, alegando descumprimento ao disposto nesta Lei.	Entendemos que esse parágrafo 1º não faz sentido. Se a própria lei dispensa o consentimento, não há descumprimento.
§ 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.	As circunstâncias nem sempre permitem que a providência seja "imediata" e a eficiência da medida pode variar. Por isso, a palavra "imediata" pode ser substituída por "prazo razoável", cabendo à autoridade competente avaliar tal razoabilidade, de acordo com a situação concreta.
§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2o, o responsável enviará ao titular, em até sete dias a partir da data do recebimento da comunicação, resposta em que poderá:	
I – comunicar que não é agente de tratamento dos dados; ou	Em complemento a essa previsão, sugerimos que nesse caso seja também indicar, se possível, quem seria o agente de tratamento de dados.
II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 4º A providência de que trata o § 2o será realizada sem ônus para o titular. § 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento. Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular: I – em formato simplificado, imediatamente; ou	
II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.	Sugerimos que a palavra "*imediatamente*" e o termo "*prazo de até sete dias*" sejam modificados para "*em prazo razoável*", já que essa razoabilidade depende de circunstâncias diversas.
§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.	Sugerimos a remoção do parágrafo 1º do art. 18. Se o formato for incompatível com o cumprimento da obrigação, o descumprimento da lei já é uma decorrência lógica. Por outro lado, o dispositivo abre a possibilidade de imposição de formatos ao responsável pelo tratamento.
§ 2º As informações e dados poderão ser fornecidos, a critério do titular:	Sugerimos a remoção do parágrafo 2º do art. 18, uma vez que a definição da melhor forma deve ser dada pelo responsável pelo tratamento, de acordo com as circunstâncias, desde que permita ao titular o efetivo acesso à informação requerida.
I – por meio eletrônico, seguro e idôneo para tal fim; ou II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.	

§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.	
§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.	Sugerimos a remoção do parágrafo 4º do art. 18, uma vez que a definição da melhor forma deve ser dada pelo responsável pelo tratamento, de acordo com as circunstâncias, desde que permita ao titular a efetiva compreensão da informação requerida.
Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.	Entendemos que este artigo 19 fere o direito à liberdade de contratação, uma vez que dá a uma das partes a possibilidade de interferir no juízo de valores e avaliação de riscos da outra.
§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.	Além de ferir a liberdade de contratação, conforme quadro acima, este dispositivo afronta o direito constitucional ao segredo de negócio, uma vez que tais critérios e procedimentos são bens imateriais, sigilosos e perdem seu valor e eficácia quando revelados.
§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal.	
Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.	Entendemos que não há razão para tal vedação caso os dados sejam corretos, pois poderia prejudicar terceiros, que seriam impedidos de utilizar informação relevante. Para sanar o problema, sugerimos a inclusão da palavra "*ilicitamente*" antes de "*utilizados*".
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.	
CAPÍTULO IV – COMUNICAÇÃO E INTERCONEXÃO	
Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados. Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.	
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.	O artigo é desnecessário já que repete a definição e conceitos já dispostos na Lei. Caso seja mantido, sugerimos que a redação seja alterada para: *"Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei"* .
Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo: I – nas hipóteses de dispensa do consentimento previstas nesta Lei;	
II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou	O disposto no inciso II do art. 24 se repete ao longo do texto e reflete uma permissividade excessiva de compartilhamento de dados entre órgãos públicos, resultando em um desequilíbrio entre obrigações do setor privado e do setor público, deixando o titular de dados pessoais vulnerável diante do Estado.
III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.	O inciso dá grande poder discricionário à autoridade competente, permitindo a ela avaliar exceções de interesse público. Por isso, é importante ter clareza quanto aos poderes, composição e natureza da autoridade.

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. Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo. 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.	
Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.	A forma com que esta redação se apresenta dá ao órgão regulador poderes de legislador. É importante delimitar os poderes regulatórios a aspectos técnicos, respeitados os termos da lei.
CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS	
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:	O modelo proposto para a transferência internacional de dados, em que é permitida apenas a países com o mesmo nível de proteção legal a dados pessoais, é inspirado no modelo europeu. Tal modelo é amplamente criticado e já está sob revisão por demonstrar-se ineficiente. A tentativa de erguer barreiras geográficas em um ambiente de rede mundial é incompatível com a configuração da Internet. Não raro, os mesmos dados são transferidos e armazenados em diferentes bancos de dados, que podem se localizar em países distintos. Decisões relacionadas à transferência e armazenamento de dados atendem, sobretudo, a requisitos técnicos, para melhor aproveitamento da infraestrutura disponível, o que, ao final, reverte-se em benefício ao usuário da Internet. Ainda, consideramos que o mecanismo das cláusulas contratuais gerais para a transferência internacional de dados pode vir a ser limitador para a transferência de dados das empresas, dado que os fluxos de dados e a atividade econômica são verdadeiramente globais por natureza. Assim, defendemos a inclusão de mecanismos de transferência internacional de dados, tal como por exemplo, o sistema APEC Cross-Border Privacy Rules desenvolvido pela Cooperação Econômica Asia-Pacífico (APEC), o qual permite garantir a proteção de dados pessoais nas
I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional; II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;	
III – quando órgão competente autorizar a transferência, nos termos de regulamento;	O inciso III do art. 28 confere à autoridade competente o poder discricionário para regulamentar as hipóteses em que a transferência pode ser autorizada, independente da legislação do país-sede do receptor de dados. A nebulosidade que cerca a autoridade competente traz enorme insegurança, já que tais autorizações podem ficar sujeitas a critérios inadequados.
IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;	
V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.	O inciso V do art. 28 traz ao titular de dados grande insegurança, já que o deixa vulnerável diante do Governo, que pode definir arbitrária e unilateralmente a transferência de dados pessoais, sem revisão dos demais Poderes. A indefinição quanto à estrutura da autoridade competente.

Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:	A sujeição da transferência internacional de dados à análise do marco regulatório de países estrangeiros por uma autoridade competente resulta, como a experiência europeia demonstra, em burocracia que torna inexequível a aplicação desse critério.
I – normas gerais e setoriais da legislação em vigor no país de destino; II – natureza dos dados; III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;	
IV – adoção de medidas de segurança previstas em regulamento; e	A sujeição de autorização ao atendimento de medidas de segurança previstas em regulamento, conforme inciso IV, indica a possibilidade do órgão competente definir normas que resultam em ingerência na estrutura de segurança de empresas, complexas e, muitas vezes incompatíveis com medidas isoladas. Ademais, tais estruturas, para a segurança dos próprios titulares de dados pessoais, normalmente são sigilosas. Além disso, questões de segurança devem ser previstas expressamente em lei e não em regulamento. Todo o texto da lei indicia ou delega a a regulação das questões mais sensíveis dos dados pessoais ao executivo, o que é um grave risco aos direitos fundamentais.
V – outras circunstâncias específicas relativas à transferência.	
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:	O consentimento à transferência internacional pelo titular, dado nos termos já definidos na Lei, deve ser suficiente para autorizá-la. A própria estrutura da Lei, atribuindo responsabilidade solidária e objetiva a quem transmite e a quem recebe dados (art. 31), já protege o titular, que normalmente não poderá compreender detalhes técnicos relacionados a possível vulnerabilidade atribuída à legislação de um país estrangeiro.
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.	
Art. 30. A autorização referida no inciso III do caput do art. 28 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.	
§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário. § 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular. § 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.	Este artigo e seus parágrafos atribuem à autoridade competente, para a autorização da transferência internacional de dados, poder absoluto de ingerência no negócio dos responsáveis pelo tratamento de dados. Isso inclui a capacidade de interferir na estrutura contratual desses responsáveis com seus usuários, bem como aos termos globais de uso de seus serviços, podendo obrigar mudanças e inclusão de cláusulas-padrão. Tal nível de ingerência afronta o princípio constitucional da livre iniciativa, além de, mais uma vez, colocar em risco o segredo de negócios, ao prever a possibilidade de realizar diligências de verificação.
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.	Este artigo prevê a responsabilidade solidária e objetiva, exclusivamente quanto à transferência de dados. Mais à frente, a Lei estabelece responsabilidade subjetiva aos agentes, nas demais formas de tratamento.

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.	O artigo 32 também burocratiza o tratamento de dados quando a transferência internacional ocorre no fluxo em que o Brasil é o receptor. Para tratar dados transferidos de outro país, o responsável pelo tratamento terá que analisar as normas do país e sua aplicação quanto ao consentimento. Sugerimos a sua eliminação, dado que a redação deste artigo traz responsabilidade adicional para o agente brasileiro no sentido, de este ter que passar a avaliar e tutelar o cumprimento das regras de proteção de dados em outros Países, tornando-o num "agente de polícia" do cumprimento da legislação estrangeira, em relação a dados que nem sequer são de cidadãos brasileiros. Nestes moldes, tal disposição trará mais onerosidade para as empresas brasileiras.
Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.	
CAPÍTULO VII – RESPONSABILIDADE DOS AGENTES	
Seção I – Agentes do Tratamento e Ressarcimento de Danos	
Art. 34. São agentes do tratamento de dados pessoais o responsável e o operador.	
Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo. § 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa; § 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.	Como regra geral, a configuração da responsabilidade civil pressupõe, além do dano e do nexo causal, um ato ilícito praticado pelo agente (art. 927, caput, CC), consubstanciado na violação intencional ou culposa de um direito alheio (art. 186, CC), ou no exercício abusivo do próprio direito (art. 187, CC). A responsabilidade civil prescinde de culpa quando a atividade normalmente desenvolvida pelo agente implicar, por sua natureza, risco para diretos de outrem (art. 927, p. único, CC), e nas demais hipóteses expressamente previstas em lei, como a ocorrência de dano causado a consumidor por defeito do serviço (art. 14, CDC). A redação do artigo 35 estabelece uma modalidade de responsabilidade civil ainda mais ampla, em que não se exige a ocorrência de ilícito (por dolo ou culpa), tampouco de defeito no serviço. Dentre inúmeras hipóteses de responsabilização civil decorrentes de atos de maior gravidade – como erros médicos e acidentes de trânsito – não parece adequado ou justificável que a lei confira tal abordagem ao dano decorrente do tratamento de dados pessoais. Seria mais apropriado o estabelecimento da responsabilidade civil dos agentes do tratamento de dados pessoais seguindo a sistemática já adotada pelos Códigos Civil e de Defesa do Consumidor. Também não se mostra adequada ou justificável a inversão do ônus da prova quando sua produção “pelo titular resultar excessivamente onerosa”, conforme previsto no § 1º do artigo 35. A onerosidade excessiva da produção da prova poderia justificar - sob uma perspectiva de causa e efeito - a imputação ao agente do tratamento de dados pessoais da obrigação de arcar com as despesas e custos da prova, mas não a inversão do ônus de produzi-la (que inclui o pedido justificado de produção e a delimitação de seu objeto).
Art. 36. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. Art. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, conforme disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992. 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.	
Seção II – Responsável e Operador	
Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.	Consideramos que a redação dos arts. 39 a 47 prevêem obrigações que parecem aplicar-se a ambos o responsável e ao operador, contudo, isto gera incerteza e obrigações conflitantes para os dois, responsáveis e operadores no Brasil. Ainda que as definições dos dois agentes (responsável e operador) estejam claras no Artigo 5 deste Anteprojeto de Lei, na prática a redação, por exemplo, do Artigo 42 prevê que as medidas de segurança sejam adotadas pelo operador quando não é este o responsável pelo tratamento de dados e sim o responsável, devendo sim o operador ficar sujeito às determinações do responsável em relação às medidas de segurança . Deste modo, sugerimos que todos os artigos acima indicados sejam revistos para serem aplicáveis aos responsáveis pelo tratamento dos dados.

§ 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.	O § 1º do artigo 39 deve ter a sua redação aprimorada para deixar claro que o responsável tem responsabilidade solidária perante o titular quanto a todas as operações de tratamento realizadas pelo operador, assegurado ao responsável o direito de regresso contra o operador, inclusive para fins de denunciação da lide. Esse ajuste, além de prestigiar o direito de regresso, tem o efeito de contribuir para que não apenas o responsável (em tese mais exposto a demandas dos titulares), mas também o operador atue em conformidade com as normas aplicáveis à matéria. Não o fazendo, pode ser responsabilizado não só pelo titular, diretamente, como também pelo responsável, em regresso.
§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.	
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.	A obrigação de manutenção de registro das operações de tratamento de dados pessoais, prevista no artigo 40, pode implicar, a depender de seu delineamento, excessiva intervenção na esfera da privacidade e intimidade dos titulares. O registro das operações de tratamento de dados pessoais, que são realizadas, como previsto na própria lei, segundo consentimento livre, expresso, específico e informado do titular, é capaz de indicar, dentre outros elementos, suas atividades, opções e preferências, muitas delas de cunho íntimo. O registro das operações de tratamento de dados pessoais, que são realizadas, como previsto na própria lei, segundo consentimento livre, expresso, específico e informado do titular, é capaz de indicar, dentre outros elementos, suas atividades, opções e preferências, muitas delas de cunho íntimo. Para exemplificar, o titular que se registra em uma rede social voltada a encontros amorosos pode consentir que seus dados pessoais sejam exibidos pelo responsável a pessoas do mesmo sexo, sem pretender que isso venha a se tornar de conhecimento do público. A obrigatoriedade de manutenção do registro dessa operação de tratamento em específico pode não apenas contrariar interesse do próprio titular, como também expô-lo ao risco de divulgação da respectiva atividade a terceiros, em decorrência, por exemplo, do cumprimento de ordem judicial imposta ao responsável. A fim de afastar essa hipótese, o artigo 40 deve excluir expressamente a obrigatoriedade de registro, pelo responsável ou operador, de operações de tratamento de dados pessoais que sejam passíveis de identificar atividades, opções, preferências e outros aspectos da privacidade e intimidade do titular, em relação aos quais ele não tenha consentido com o referido registro. Além disso, também com o propósito de assegurar a inviolabilidade da privacidade e intimidade do titular, o artigo 40 deve estabelecer de forma expressa um prazo máximo de manutenção dos registros, a exemplo do que prevê a Lei 12.965/2014 (Marco Civil da Internet) quanto à guarda de registros de conexão e de acesso a aplicações de internet.
Parágrafo único. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.	
Seção III - Encarregado pelo Tratamento de Dados Pessoais	
Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.	A exigência de indicação, pelo responsável, de um encarregado pelo tratamento de dados pessoais, com a atribuição, inclusive, de receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, parece não considerar o volume de demandas dessa natureza recebidas por empresas de grande porte. Em vez de contribuir para o melhor atendimento do titular, a previsão do artigo 41 pode torná-lo inviável ou ineficaz, por concentrar em um encarregado atribuições para as quais pode ser necessário um departamento com dezenas ou até centenas de pessoas. Tais atribuições devem ser imputadas, portanto, ao responsável, seja pessoa física ou jurídica, sem a obrigatoriedade (mas, em vez disso, apenas a opção) de indicação de um encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet. § 2º As atividades do encarregado consistem em:	

I - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações do órgão competente e adotar providências; III - orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - demais atribuições estabelecidas em normas complementares ou determinadas pelo responsável. § 3º Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.	
Seção IV – Segurança e Sigilo dos Dados	A Seção IV aborda padrões de segurança e sigilo de dados que posteriormente deverão ser objeto de regulamentação específica, inclusive por órgão competente a ser criado para tal finalidade. O principal objetivo da seção é criar alguns parâmetros a serem seguidos em casos de incidentes de segurança que gerem "vazamento" de dados pessoais, bem como medidas para mitigar seus efeitos, de forma a minimizar os danos dos titulares de dados pessoais. A seção não prevê qual será o órgão competente para exercer a fiscalização das medidas de segurança, o que deverá ser objeto de futura regulamentação.
Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito. Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.	O artigo prevê de forma genérica a obrigação do operador de adotar medidas de segurança visando impedir acessos não autorizados ou incidentes de segurança conhecidos como "vazamento" de dados pessoais. Tais medidas não se limitam ao aspecto técnico propriamente dito, contemplando também providências administrativas, como, por exemplo, a imposição de obrigação contratual de confidencialidade aos funcionários do operador, normas e políticas internas, bem como medidas de fiscalização pelo operador. Embora não elimine a necessidade de regulamentação, o parágrafo único estabelece parâmetros mais específicos para as medidas de segurança, em especial "o atual estado da tecnologia". Esse parâmetro poderá representar desestímulo em determinados setores devido aos altos custos envolvidos no emprego de medidas compatíveis com o atual estado da tecnologia. Ademais, já se verifica que a extensão dessa obrigação sofrerá inúmeras variações dependendo da natureza dos dados e das características específicas do tratamento, demandando uma regulamentação detalhada.
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.	O artigo impõe àqueles que de qualquer forma participem do tratamento uma obrigação de manterem o sigilo dos dados pessoais. Tal obrigação não apresenta qualquer limitação temporal, permanecendo vigente mesmo após o término do tratamento. Embora a obrigação seja atribuída diretamente aos agentes de tratamento, caberá ao operador zelar pelo cumprimento dessa obrigação por todos aqueles que dele participem de alguma forma, recomendando-se a criação de políticas internas e celebração de termos específicos para tanto.
Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares. Parágrafo único. A comunicação deverá mencionar, no mínimo: I – descrição da natureza dos dados pessoais afetados; II – informações sobre os titulares envolvidos; III – indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;	O artigo obriga que quaisquer incidentes que afetem a segurança de dados sejam imediatamente comunicados ao órgão competente, inclusive mediante o fornecimento de informações que permitam avaliar a sua gravidade e riscos, os dados afetados e as medidas já adotadas ou planejadas para reverter ou mitigar prejuízos. O grande número de informações a serem fornecidas ao órgão competente poderá eventualmente inviabilizar uma comunicação imediata, já que em determinados casos haverá necessidade de se apurar em maiores detalhes os fatos e as medidas cabíveis para minimizar riscos.

IV – riscos relacionados ao incidente; e V – medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.	Diante disso, sugere-se que a comunicação acerca do incidente seja imediata, estabelecendo-se um prazo razoável para fornecimento de informações adicionais que eventualmente não possam ser apresentadas de imediato.
Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como: I – pronta comunicação aos titulares; II – ampla divulgação do fato em meios de comunicação; ou III – medidas para reverter ou mitigar os efeitos de prejuízo. § 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los. § 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.	O artigo estabelece as medidas que poderão ser determinadas pelo órgão competente ao ser comunicado a respeito de incidentes de segurança relacionados a dados pessoais. Ao prever que tais medidas serão determinadas "conforme sua gravidade", o dispositivo impõe a observância aos princípios da proporcionalidade e da razoabilidade, de acordo com as circunstâncias específicas do caso concreto. Dessa forma, medidas drásticas como a ampla divulgação do fato em meios de comunicação deverão ser restritas a casos excepcionais e que possam de fato causar grande prejuízo aos titulares. Do contrário, a pronta comunicação aos titulares e medidas para reverter ou mitigar prejuízos serão suficientes. A adoção de medidas técnicas que tornem os dados ininteligíveis deverá ser considerada no juízo de avaliação da gravidade do incidente a fim de atenuar as medidas determinadas pelo órgão competente. Ademais, considerando que as medidas serão determinadas pelo órgão competente sempre em conformidade com a gravidade do incidente, outras circunstâncias atenuantes poderão ser consideradas para tanto, como, por exemplo, o acesso parcial a dados pessoais. Independentemente da determinação pelo órgão competente, o § 2º prevê a obrigatoriedade de pronta comunicação aos titulares afetados pelo incidente nos casos em que haja risco à sua segurança pessoal ou que possam lhes causar danos. No entanto, nos parece que todos os incidentes de segurança envolvendo dados pessoais poderão causar danos aos titulares, ainda que em grau variável. Caso o artigo não sofra modificação, a obrigatoriedade de pronta comunicação aos titulares afetados tornar-se-á verdadeira regra geral em hipóteses de incidentes de segurança envolvendo dados pessoais. O artigo não prevê o teor ou as informações que deverão ser fornecidas aos titulares por meio da comunicação. Quando a comunicação aos titulares for determinada pelo órgão competente, esse próprio órgão poderá esclarecer as informações que serão fornecidas na comunicação aos titulares. No entanto, como já referido, o artigo parece tornar regra a hipótese de pronta comunicação independentemente de determinação pelo órgão competente, tornando necessário, pois, estabelecer quais informações serão fornecidas aos titulares afetados. O ideal seria que as mesmas informações fornecidas ao órgão competente também fossem objeto da comunicação aos titulares, a fim de que possam receber informações precisas sobre os riscos e prejuízos que lhe afetem e medidas que serão adotadas pelo responsável.
Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares. Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.	Conforme já referido, as obrigações previstas nesta seção quanto às medidas de segurança são genéricas, o que demanda efetiva regulamentação acerca dos critérios e padrões mínimos de segurança aplicáveis conforme a natureza dos dados e as características específicas do tratamento. Tais normas, padrões e critérios deverão ser periodicamente revisados e atualizados com base na evolução tecnológica.
Seção V – Boas Práticas	
Art. 48. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados. Parágrafo único. As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.	Para que a formulação de boas práticas seja efetivamente incentivada, a lei deveria prever algum tipo de benefício para a entidade que as tiver como, por exemplo, a atenuação de sanções administrativas. Sugestão de inclusão de parágrafo: "*A formulação, publicação e adoção de boas práticas no tratamento de dados pessoais, nos termos do caput deste artigo, deverão ser consideradas como atenuante na hipótese de aplicação de qualquer das sanções administrativas previstas nesta Lei* .".

Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento.	De acordo com os arts. 48 e 49, a possibilidade de reconhecimento e divulgação de boas práticas e padrões de software pelo governo poderá se restringir somente às regras e padrões que implementem a legislação. Esse regime, em princípio, não abre espaço para uma autorregularão autônoma do setor voltada para a inovação. Por isso, sugerimos a inversão do princípio por trás desse artigo, para que o reconhecimento possa ser dado também a boas práticas e padrões que não sejam incompatíveis com a legislação e regulamentação.
CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS	A imposição de sanções administrativas na forma abaixo parece extrema em relação ao tipo de infração cometida e de difícil comparação com a regulação existente em outros países. A multa e a publicização, sem prejuízo do dever de indenizar e da responsabilidade de natureza penal parecem suficientes para coibir as infrações relacionadas à esta Lei.
Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente: I – multa simples ou diária; II – publicização da infração;	O artigo 2o deste APL abrange pessoas jurídicas de direito público ou privado, assim, também deverão ser previstas sanções para pessoas jurídicas de direito público que desrespeitarem a lei.
III – dissociação dos dados pessoais;	A dissociação pode se mostrar tecnicamente impossível. Sugestão de retirada do termo ou de inclusão do termo "*desde que tecnicamente possível no sistema utilizado para o tratamento de dados"*.
IV – bloqueio dos dados pessoais;	Termo vago e que implica a impossibilidade da livre realização de atividade econômica. Sugerimos sua retirada, sob pena de ser objeto de questionamento judicial.
V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;	Implica a impossibilidade da livre realização de atividade econômica. Sugerimos sua retirada, sob pena de ser objeto de questionamento judicial.
VI – cancelamento dos dados pessoais;	Termo vago e que implica a impossibilidade da livre realização de atividade econômica. Sugerimos sua retirada, sob pena de ser objeto de questionamento judicial.
VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e	Implica a impossibilidade da livre realização de atividade econômica. Sugerimos sua retirada, sob pena de ser objeto de questionamento judicial.
§ 1º As sanções poderão ser aplicadas cumulativamente.	Sugerimos a inclusão do seguinte termo: "na hipótese de reincidência".
§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento. § 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.	Em vista dos comentários acima, sugerimos sua retirada do texto.
§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.	
§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.	Sugerimos que os incisos sejam os de I a II. Se permanecerem apenas os demais, em vista dos comentários acima, sugerimos sua retirada do texto.
CAPÍTULO IX – DISPOSIÇÕES TRANSITÓRIAS E FINAIS	
Art. 51. Órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento, a natureza dos dados e o porte do responsável.	

Art. 52. Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.	