COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI Nº 4060, DE 2012

(TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS)

PROJETO DE LEI Nº 4.060, DE 2012

(Apenso PLs nºs 5.276/16 e 6.291/16)

Dispõe sobre o tratamento de dados pessoais, e dá outras providências.

Autor: Deputado MILTON MONTI
Relator: Deputado ORLANDO SILVA

I – RELATÓRIO

Tramita nesta Comissão, em regime ordinário, sujeito à apreciação do Plenário da Câmara dos Deputados, o Projeto de Lei (PL) nº 4.060, de 2012, de autoria do Deputado Milton Monti, dispondo sobre o tratamento de dados pessoais. Apensos à proposição principal encontram-se os PLs 5.276/16, do Poder Executivo, e 6.291/16, do Dep. João Derly.

O projeto principal, do Dep. Milton Monti, é dividido em três capítulos, que agrupam vinte e cinco artigos, dos quais o primeiro, que trata de disposições gerais, enuncia os princípios norteadores, estabelece as definições legais e delimita o escopo de abrangência, que é o tratamento de dados pessoais realizado em território nacional, ainda que o banco de dados esteja armazenado em território estrangeiro.

O segundo Capítulo da proposta trata dos requisitos para tratamento dos dados pessoais, exigindo que os responsáveis pelo tratamento dos dados adotem medidas tecnológicas, proporcionais ao estado da tecnologia, que minimizem os riscos de acesso não autorizado ou de perda dos dados dos titulares. Os dados pessoais poderão ser processados respeitada a lealdade e a boa fé e observado o legítimo interesse dos titulares.

No que respeita aos dados sensíveis – definidos no texto como aqueles relativos à origem social e étnica, à informação genética e outros aspectos pessoais – o tratamento dessas informações em bancos de dados públicos ou privados só poderá ocorrer mediante prévia autorização do titular. Ademais o seu repasse a terceiros poderá ser bloqueado mediante manifestação direta ao responsável.

O terceiro e último Capítulo, relaciona o direito dos titulares dos dados de requerer, a qualquer momento, o bloqueio do tratamento de suas informações pessoais, assim como seu amplo acesso à política de privacidade dos responsáveis pelo tratamento.

No mesmo Capítulo III, o Título II trata da tutela fiscalizatória e sancionatória, dispõe sobre as penalidades e sanções ao descumprimento das disposições da lei. Ademais, o dispositivo abre a possibilidade de criação de conselhos de autorregulamentação da matéria por parte das instituições representativas de entidades do setor.

O Projeto de Lei apenso, PL nº 5.276/16, de autoria do Poder Executivo, trata do tema de maneira mais extensiva. Possui 56 artigos, divididos em nove capítulos. O projeto é de iniciativa do Ministério da Justiça, que coordenou o processo de elaboração e de consulta junto à população. Conforme Mensagem da Presidência da República, a proposta é fruto da Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital". A Mensagem informa ainda que "109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema".

No Capítulo I, "Disposições Preliminares", são delimitados o escopo da Lei, seus fundamentos, exceções, definições e princípios. São definidos como dados sensíveis aqueles que tratem da "origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos" (Art. 5º, III).

O Capítulo II, "Requisitos para o Tratamento de Dados Pessoais", determina que o tratamento de dados somente pode ser realizado mediante "consentimento livre, informado e inequívoco pelo titular" (Art. 7º, I). Já para dados sensíveis, o tratamento somente poderá ser realizado mediante "consentimento livre, inequívoco, informado, expresso e específico" (Art. 11, I).

São asseguradas as condições em que o Poder Público poderá tratar dados sem consentimento para os casos previstos em Lei. É permitido o tratamento de dados de crianças e adolescentes “no seu melhor interesse, nos termos da legislação pertinente” (Art. 14).

O Capítulo III, “Dos Direitos do Titular”, garante ao titular o acesso, correção, anonimização, portabilidade e eliminação dos dados pessoais (Art. 18). Com relação a dados que tenham sido tratados de forma automática, o titular poderá “solicitar revisão das decisões tomadas” (Art. 20).

O Capítulo IV, “Do Tratamento de Dados Pessoais Pelo Poder Público”, determina, como regra geral, que a transferência de dados pessoais, de entidade pública para privada, deverá ser informada ao órgão competente e dependerá de consentimento do titular (Art. 27). Órgão competente poderá requerer “relatórios de impacto de privacidade e poderá sugerir a adoção de padrões e boas práticas” (Art. 32).

O Capítulo V, “Da Transferência Internacional de Dados”, estabelece que esse tipo de transferência somente poderá se dar para países que possuam a mesma proteção legal ou em casos judiciais, criminais, de proteção à vida ou, ainda, para o atendimento a acordos e mediante consentimento (Art. 33).

O Capítulo VI, “Dos Agentes do Tratamento de Dados Pessoais”, define os distintos agentes envolvidos com tratamento de dados: responsável; operador e encarregado (Art. 41). Determina, também, que todos os envolvidos com tratamento de dados têm obrigação de reparar dano patrimonial, moral, individual ou coletivo (Art. 42).

O Capítulo VII, “Da Segurança e Das Boas Práticas”, determina ao operador a adoção de boas práticas (Art. 45), a serem definidas pelo responsáveis (Art. 50). Cabe a esse último a comunicação ao órgão competente acerca de incidentes de segurança (Art. 46) e a esse tomar medidas para reverter ou mitigar os efeitos do sinistro (Art. 48).

O Capítulo VIII, “Da Fiscalização”, dispõe sobre as sanções administrativas, estas progressivas, desde multa simples a suspensão do funcionamento de banco de dados (Art. 52). É prevista a designação de órgão competente “para zelar pela implementação e pela fiscalização” da Lei (Art. 53), bem como a criação de um Conselho Nacional de Proteção de Dados

Pessoais e da Privacidade que será composto por quinze representantes (Art. 54), com função consultiva.

Também apenso está o PL nº 6.291/17, de autoria do Deputado João Derly, que propõe alterar o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de internet com terceiros. A proposição possui três artigos e cria o direito ao não compartilhamento, exceto mediante consentimento livre, inequívoco, informado, expresso e específico pelo titular. O projeto se vale de conceitos similares para a definição de dados pessoais e de dados sensíveis aos contidos no PL nº 5.276/16, e prevê sanções, no Marco Civil, para a violação de direitos do titular.

Esse é o relatório quanto aos projetos ora em análise.

O PL principal, foi distribuído originalmente para análise de mérito às Comissões de Ciência e Tecnologia, Comunicação e Informática (CCTCI), de Trabalho, de Administração e Serviço Público (CTASP) e de Constituição e Justiça e de Cidadania (CCJC). Essa última deveria, também, se pronunciar quanto à constitucionalidade e juridicidade, respectivamente, conforme o artigo 54, do RICD. A proposição tramitava em regime ordinário e sujeita à deliberação do Plenário. Quando apensado o PL do Poder Executivo, a proposição passou a tramitar em regime de prioridade e, após novas alterações de tramitação, foi constituída Comissão Especial, em 25/10/2016. O PL do Deputado João Derly foi apensado em 27/10/2016.

O PL nº 5.276/16 recebeu 11 Emendas de Plenário, as quais relatamos:

O **Deputado Weverton Rocha** (EMP 1 a 3) propõe a alteração do Art. 50, que determina que responsáveis pelo tratamento **poderão** estabelecer regras de boas práticas, substituindo a opção por **deverão (EMP 1)**. A **EMP 2** inclui hipótese de encerramento do tratamento de dados por determinação judicial (Art. 15, V). A **EMP 3** suprime da lei o parágrafo único do artigo 16 que permite ao órgão competente estabelecer “hipóteses específicas de conservação de dados pessoais”.

O **Deputado Jorge Tadeu Mudalen** oferece a **EMP 4** que suprime o consentimento **informado** para o tratamento de dados pessoais

(Art. 7º, I e art. 9º) e o consentimento **informado, expresso e específico** para o tratamento de dados sensíveis (Art. 11).

A **EMP 5**, do **Deputado Leonardo Quintão**, **retira do responsável a obrigação de informar ao titular** acerca do tratamento de dados para cumprir obrigação legal ou pela Administração (Art. 7º, §1º).

O **Deputado Sandro Alex** apresenta a **EMP 6**, suprimindo as **atribuições do órgão responsável** de realizar auditoria, de publicizar as operações e de estabelecer normas complementares (Art. 53, III, VIII, X).

As EMP 7 a 11 foram oferecidas pelo **Deputado Paes Landim**. A **EMP 7** altera a definição de **uso compartilhado de dados** em que o tratamento poderia ser compartilhado mediante **delegação** de ente público para somente aquele em que ente público fosse **permitido** a fazê-lo (Art. 5º, XV). Ademais, a emenda determina que o uso compartilhado de dados deve atender a **todos os princípios de proteções de dados pessoais** (Art. 26, caput) e acresce a possibilidade da **transferência de dados pessoais** em caso de "**previsão legal ou respaldo em convênio celebrado com entidades privadas**, com finalidade específica" (Art. 26, parágrafo único). A **EMP 8** acresce a hipótese dos dados pessoais poderem ser tratados também para fins de **proteção de crédito** (Art. 7º, X). A **EMP 9** inclui o respeito aos **segredos comercial e industrial** quando: da informação ao titular acerca do tratamento de dados (Art. 8º, I e § 3º); o órgão competente solicitar relatório de impacto à privacidade a responsável (Art. 10, § 4º e Art. 39); do compartilhamento de dados anonimizados (Art. 13, § 3º); requerida portabilidade pelo titular (Art. 18, V), e; solicitação de cópia dos dados pelo titular (Art. 19, § 3º). A **EMP 10** altera a definição de **dados sensíveis** para determinar que **dados biométricos** somente serão sensíveis quando "**se referirem à indicação de raça ou etnia do titular**". Por fim, a **EMP 11** inclui no rol de dados pessoais aqueles "**que o processo de anonimização puder ser revertido com esforços razoáveis**" (Art. 13, § 1º).

É o relatório.

II - VOTO DO RELATOR

1. Introdução

A preocupação com a proteção dos dados das pessoas vem crescendo ao longo dos anos junto à sociedade e à esta Casa de Leis e ganhou maior destaque, especialmente, quando da aprovação do Marco Civil da Internet, instituído pela Lei nº 12.965, de 2014. Nesse contexto, o Dep. Milton Monti, autor da primeira proposta aqui analisada, transpôs para o papel preocupações extremamente pertinentes. O Deputado esclareceu a questão da tutela dos dados pessoais e a responsabilidade dos agentes de tratamento, além de cristalizar importantes conceitos tais como a necessidade de obtenção de consentimento para o tratamento de dados sensíveis e a definição clara dos procedimentos que devem pautar a interconexão de dados entre responsáveis.

A segunda proposta anexa, de autoria do Dep. João Derly, possui como cerne não permitir o compartilhamento de dados pessoais com terceiros sem o consentimento "livre, inequívoco, informado, expresso e específico" do titular. Ademais, o projeto traz para o âmbito do Marco Civil da Internet uma extensa, porém objetiva, definição do que constituem dados pessoais.

Em que pese a pertinência dessas matérias, com a apensação do PL nº 5.276/16, de autoria do Poder Executivo, temos para análise uma proposta muito mais discutida, pormenorizada e complexa. Portanto, sem maiores delongas, externo desde já que nesta análise utilizarei ideias e conceitos contidos nos três textos apresentados.

Em particular, cabe destacar que o Projeto de Lei nº 5.276/16, enviado pelo Poder Executivo, é fruto do trabalho desenvolvido durante cinco anos no Ministério da Justiça, por meio da Secretaria Nacional do Consumidor (Senacon). Segundo informações do próprio Ministério, para a elaboração da matéria foram realizados dois debates públicos pela internet, em 2010 e 2015, tendo sido recebidas mais de 2.000 contribuições dos diversos setores envolvidos. Ademais o órgão realizou diversas reuniões técnicas e setoriais.

Importante pontuar que as propostas se inserem em um contexto mundial, portanto, maior, em que legislações nacionais são

introduzidas em cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica. Ao mesmo tempo, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados. De fato, a Mensagem do Poder Executivo, ao PL nº 5.276/16, ressalta que a proposta é fruto da Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital", e que "109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema".

2. Uma breve contextualização internacional

Grande fonte de inspiração para os projetos advém do arcabouço europeu. O primeiro instrumento daquele bloco na temática é a Convenção do Conselho da Europa nº 108, de 1981, "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais".[1] O segundo instrumento geral é a Diretiva Europeia nº 46, de 1995, conhecida como Diretiva de Proteção de Dados.[2] Em terceiro lugar, citamos a Diretiva nº 58, de 2002,[3] focada na proteção da privacidade no âmbito das comunicações eletrônicas. Esse conjunto de normas está devidamente internalizado nos países que compõem o bloco.

Em 2016, o sistema europeu foi revisado com a aprovação do Regulamento nº 679, de 2016, do Parlamento Europeu e do Conselho, de 27/04/2016, que trata da proteção das pessoas naturais com respeito ao processamento de dados pessoais e ao livre movimento desses

---

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, disponível em http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37, acessado em 12/7/16.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, acessado em 12/7/16.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, acessado em 15/08/16.

dados.[4] A Regulação revoga a Diretiva 95/46 e entra em vigência em 25 de maio de 2018. O objetivo da nova regulação é dar resposta apropriada aos rápidos avanços tecnológicos e à globalização, que trouxeram novos níveis de escala da coleta e de compartilhamento de dados pessoais, inclusive transferidos internacionalmente. O novo instrumento fortalece o papel fiscalizatório dos órgãos de controle, bem como entrega às pessoas naturais o poder efetivo sobre seus próprios dados, detalhando os conceitos de transparência e de consentimento destacado. A norma adentra em questões como dados sensíveis, genéticos, anonimização e pseudonimização, legítimo interesse e tratamento global (transferência internacional) dos dados pessoais.

Já uma abordagem legislativa e regulatória diametralmente distinta é aquela adotada pelos EUA. Naquela federação a proteção de dados não possui lei específica, sendo compartilhada a regulamentação e a autoridade e competência de fiscalização entre várias instituições. Como regra geral, a privacidade é tratada como um aspecto de proteção aos consumidores e, portanto, está sob a égide da FTC (Federal Trade Commission – Comissão Americana de Comércio). Aspectos específicos encontram-se contidos nas leis de cada setor. O caso financeiro, por exemplo, é regido pelas leis de (tradução livre) Modernização dos Serviços Financeiros (Financial Services Modernization Act of 1999) e de Análise Justa de Crédito (Fair Credit Reporting Act of 1970 - FCRA). Nessa Lei de Modernização são incluídas três regras básicas com relação a dados relativos a informações financeiras pessoais: i) as instituições devem armazenar os dados de forma segura; ii) devem informar em caso de compartilhamento de informações, e; iii) devem possibilitar recusar o compartilhamento (“opt-out”).[5] A lei referente à análise de crédito (FCRA), dispõe sobre o tratamento para fins de crédito bancário e de consumo, assim como para fins de emprego. O FCRA inclui um direito à qualidade dos dados, permitindo o acesso e a correção, à segurança, limitação, destruição, aviso, consentimento e prestação de contas (*accountability*). Pelo sistema americano, o FTC comenta acerca das práticas mas não as regulamenta.

Por outro lado, dados sobre saúde, por exemplo, estão a

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679, acessado em 03/04/18.

[5] A Lei é também conhecida como The Gramm-Leach-Bliley Act (GLBA),

cargo do Departamento da Saúde e Serviços Humanos (U.S. Department of Health & Human Services) e vários desses aspectos sob a tutela da Lei que trata da portabilidade de planos de saúde (Health Insurance Portability and Accountability Act (HIPAA).[6] Com relação à proteção das crianças, a Lei dos EUA, *Children's Online Privacy Protection Act*, de 1998, conhecida como Lei COPPA,[7] possui extenso detalhamento para a proteção do grupo, que inclui, por exemplo, a notificação aos pais quando do tratamento de dados de menores.

É importante observar que durante a administração Obama, o FCC, decidiu, em 2016,[8] por impor regras de privacidade aos provedores de conexão à internet, determinando que os usuários deveriam dar consentimento expresso para o tratamento de dados sensíveis ("opt-in").[9] Já para os demais tipos de dados os provedores poderiam trata-los enquanto o titular não se manifestasse expressamente ("opt-out"). Entretanto, essa decisão foi revogada pelo Congresso norte-americano em março de 2017, com a mudança presidencial e de orientação política ocorrida naquele país.[10]

Outra decisão recente e bastante relevante foi a tomada pelo Federal Trade Commission – FTC[11] contra conhecida empresa de aplicativo para transporte de passageiros, acusada de não proteger corretamente os dados sobre seus motoristas e passageiros, violando sua privacidade. A FTC decidiu que a empresa deverá implementar abrangente programa de garantias à privacidade dos dados pessoais de seus usuários, cujo resultado será auditado de 2 em 2 anos, por um prazo de 20 anos, por

---

[6] A HIPAA é parte integrante do Código Americano, referência 42 U.S.C. §1301 et seq.

[7] Disponível em http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5, acessado em 14/07/16.

[8] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services. Report and Order (FCC 16-148). (FCC, 2016). Disponível em: https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy, acessado em 10/05/2017.

[9] FCC ADOPTS PRIVACY RULES TO GIVE BROADBAND CONSUMERS INCREASED CHOICE, TRANSPARENCY AND SECURITY FOR THEIR PERSONAL DATA (FCC, 2016). Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A1.pdf, acessado em 10/05/2017.

[10] S.J.Res.34 - A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services". (Congress, 2017). Disponível em: https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34/text, acessado em 10/05/2017.

[11] Disponível em: https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_decision_and_order.pdf , acessado em 16/08/2017.

empresa independente.

O caso de alta repercussão mundial envolvendo o Facebook e a Cambridge Analítica, embora até o presente momento seja muito cedo para analisar a extensão do problema e das consequências, é outro evento tornado a público que demandou ações de investigação não somente pelo FTC como também pelo Congresso daquele país. Esses episódios mostram que, ao contrário da percepção corrente por determinados setores, a regulação sobre a proteção de dados pessoais nos Estados Unidos, apesar de esparsa e compartilhada entre vários órgãos da administração pública, não é ausente.

Nesta contextualização internacional é importante observar que a Diretiva Europeia, extensamente detalhada e que possui 99 artigos e 173 notas explicativas, não permite a transferência internacional de dados para países que não possuam legislação que garanta a mesma proteção dada pela Lei Europeia. Por esse motivo, os EUA e o bloco possuíam, desde 2000, um entendimento, conhecido como Porto Seguro (*Safe Harbour Decision)*,[12] onde eram garantidas as proteções legais europeias, quando o tratamento de dados de cidadãos europeus fosse feito nos EUA. Entretanto, uma decisão da Corte Europeia, de 2015,[13] em caso movido pelo cidadão austríaco Max Schrems contra o Facebook, determinou a invalidez do acordo em face das revelações do caso *Snowden*. Uma vez que a falta de acordo coloca em sério risco jurídico as operações das empresas globais, particularmente as da internet, um novo acordo foi gestado e finalmente aprovado em 12 de julho de 2016 pela Comissão Europeia. O acordo, batizado de Escudo de Privacidade (*Privacy Shield*), inclui a supervisão direta do Departamento de Comércio dos EUA nas empresas que desejarem dele se valer. Tal arranjo equivale à instituição de uma autoridade nacional de proteção e a introdução de um ordenamento legal para as empresas daquele país, quando tratarem de dados de cidadãos europeus.

Outro acordo importante e que representava alternativa à

[12] A Comissão Europeia adotou a decisão (Safe Harbour) e o Departamento de Comércio dos EUA estabeleceu o EU-US Privacy Shield onde são estipuladas as exigências às quais as empresas americanas que tratarem de dados de europeus tem que aderir em atendimento ao acordo. Disponível em https://www.commerce.gov/privacyshield, acessado em 12/7/16.

[13] The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press Release 117/15, 6/10/15, disponível em http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf, acessado em 12/7/16.

regulação europeia era o TPP (Trans-Pacific Trade Partnership). Entretanto, sob a administração Trump, os EUA se retiraram da iniciativa. Procurando manter posição de destaque na temática, o restante do bloco originário do TPP apresentou a alternativa CPTPP (Acordo Abrangente e Progressivo para Parceria Trans-Pacífica). O instrumento conta com a participação dos 11 países restantes, entre eles Canadá, México, Japão, Austrália e Chile. O Japão, a propósito, é considerado um país com proteção de dados robusta e madura, possui Lei e autoridade específica e procura ser um contraponto global na temática.

Nesta análise não poderia se deixar de lado uma menção à China. Força emergente da região e do mundo, o país é reconhecido por ter o tráfego de internet extremamente supervisionado e protegido. Por isso, possui autoridade focada em *cybersegurança*. Já com relação ao arcabouço regulatório de proteção de dados, as disposições são decentralizadas, como no sistema dos EUA.

Passando ao exame das similaridades das propostas ora em análise com o arranjo regulamentar e institucional de países mais próximos, verificamos que a Argentina possui sua Lei de Proteção dos Dados Pessoais (Lei nº 25.236), desde o ano de 2000. Naquele país foi instituída a autoridade reguladora, *Dirección Nacional de Protección de Datos Personales*, e, segundo suas próprias informações, é o primeiro país Latino-americano a ganhar a certificação da União Europeia como “país adequado”, em referência ao atendimento às disposições daquele bloco.

Esse ponto, de a legislação do país estar de acordo com a legislação europeia, é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de *data centers*, mas das próprias empresas de TIC, incluindo as gigantes *ponto com*. Por isso, a necessidade de o Brasil possuir, sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia.

Outra questão essencial, presente nas leis de vários

países, e que se coloca na proposição legislativa brasileira, é a de que espécie de responsabilidade por ato ilícito deveria recair sobre os agentes que realizam atividades de tratamento de dados pessoais. Neste particular, a responsabilidade civil possui diferentes tratamentos de acordo com cada país. A União Europeia, por exemplo, determina que haja responsabilidade do Responsável[14] independente de culpa, mas não do Operador[15], que só responderá na hipótese em que transgredir obrigações específicas a ele direcionadas ou agir contrariamente às instruções legítimas do Responsável[16]. A legislação brasileira adota a regra geral de responsabilidade objetiva, aquela que independe de culpa do infrator, quando há relação de consumo (conforme o Código de Defesa do Consumidor, arts. 7º e 12). E também há responsabilidade objetiva quando a atividade desenvolvida é considerada de risco, como podem ser consideradas as atividades relacionadas ao tratamento de dados pessoais (conforme o Código Civil, parágrafo único do art. 927). Cabe perquirir se esse tratamento é o mais adequado ou se haveria exceções possíveis a ensejar reponsabilidade subjetiva em alguma parte da cadeia de valor que congrega as atividades de tratamento de dados pessoais.

Feitas estas considerações iniciais, passamos ao teor das principais discussões realizadas durante as audiências públicas e seminários no âmbito da Comissão Especial a cargo do PL nº 4.060/12.

3. Audiências Públicas e Seminários

Tendo em vista a complexidade da matéria, os relatores ao PL do Poder Executivo, quando tramitando em separado à proposição principal, entenderam pela necessidade de colher sugestões e contribuições dos principais atores envolvidos.

Assim, em 07/07/16 esta Comissão realizou Seminário conjunto com a CTASP (Comissão de Trabalho, de Administração e Serviço

[14] Por Responsável entende-se, conforme definido no art. 5º do PL nº 5.276/16, a pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
[15] Por Operador entende-se, conforme definido no art. 5º do PL nº 5.276/16, a pessoal natural ou jurídica, de direito público ou privado, que realiza tratamento de dados pessoais em nome do responsável.
[16] Para mais detalhes, ver art. 82 do Regulamento 679/2016.

Público) para debater o PL nº 5.276/16. Foram convidados Igor Rodrigues Britto, Coordenador Geral de Estudos e Monitoramento de Mercado da Secretaria Nacional do Consumidor do Ministério da Justiça – SENACON; Vladimir Barros Aras, Procurador Regional da República e Secretário de Cooperação Internacional do Ministério Público Federal; Carol Conway, Presidente do Conselho de Estudos Jurídicos da Associação Brasileira de Internet – ABRANET; Sergio Paulo Gallindo, Presidente Executivo da Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação – BRASSCOM; Paulo Renà da Silva Santarém , jurista e fundador do Instituto Beta para Internet e Democracia representando Coding Rights; Rafael Zanatta, Pesquisador de telecomunicações do Instituto Brasileiro de Defesa do Consumidor – IDEC; Antônio Carlos de Toledo Negrão, Diretor Jurídico da Federação Brasileira de Bancos - FEBRABAN/CNF; Efraim Kapulski, Presidente da Associação Brasileira de Marketing Direto – ABEMD; Mário Viola, especialista em proteção de dados pessoais e consultor da Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização – CNSeg; Sérgio Amadeu da Silveira, representante da ACTANTES; Bruno Bioni, pesquisador do Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação - GPOPAI/ USP; Marília de Aguiar Monteiro, pesquisadora do Projeto "Privacidade Brasil" Vanessa Butalla, Diretora da Associação Nacional de Bureaus de Crédito; Caio César Carvalho Lima, professor da Escola Paulista de Direito (EPD) e da Faculdade de Informática e Administração Paulista (FIAP) Informações de Apoio.[17] Todos os participantes ressaltaram a necessidade de aprovação do Projeto e quase a totalidade apresentou sugestões de aprimoramentos ao texto originalmente encaminhado.

Em 6/12/16 foi realizada audiência pública com a presença de representantes da Brasscom, Universidade Estadual do Rio de Janeiro e a Coordenadora de Análise e Orientação Técnica em Defesa do Consumidor, representando o Senacon (Secretário Nacional do Consumidor do Ministério da Justiça).[18] A representante da Brasscom destacou a necessidade de excetuar do conceito de dados sensíveis aqueles já tornados públicos pelo

[17] O resultado do Seminário, bem como pauta, vídeo e áudio podem ser verificados na íntegra em: http://www.camara.leg.br/internet/ordemdodia/ordemDetalheReuniaoCom.asp?codReuniao=44364, acessado em 7/7/16.

[18] O resultado da Audiência Pública pode ser vista em: http://www.camara.leg.br/internet/ordemdodia/ordemDetalheReuniaoCom.asp?codReuniao=46016, acessado em 08/12/16.

titular; que o consentimento deve estar harmonizado com o Marco Civil da Internet; que a transferência internacional não pode depender de chancela de outros países – uma questão de soberania; que há outros modelos de órgão regulador como nos países da APEC, que possuem uma entidade certificadora ou o Canadá; que a responsabilidade entre cedentes e cessionários deveria ser não-solidária, e, por fim; que as penas no PL estão muito severas. O professor da UERJ destacou que o foco da nova lei é a proteção de pessoas naturais; que não deveria se aplicar para fins exclusivamente pessoais; que o princípio dos dados anonimizados é de que possam ser utilizados livremente, e, finalmente; que o novo instrumento deveria ser uma Lei Geral para todos os setores. Por último, a representante do Senacon destacou que os dados pessoais deveriam se referir a pessoas determináveis; que há imprecisão na definição do que seja esforço razoável para a anonimização dos dados; que o legítimo interesse deve ser secundário a consentimentos inicialmente dados e em especial para proteções fundamentais, tais como menores de idade, e, finalmente; que o princípio da responsabilidade objetiva e solidária está cristalizado na legislação, haja vista o Código de Defesa do Consumidor.

A Audiência Pública realizada em 14/12/2016, contou com a presença de representante do Intervozes e pesquisadores do GPoPAI/USP - Grupo de Pesquisa em Políticas Públicas de Acesso à Informação e do Instituto Brasileiro de Defesa do Consumidor – IDEC. O pesquisador do grupo da USP salientou a importância da definição de dados pessoais sob a ótica expansionista, a mais utilizada no mundo, inclusive nas diretrizes da APEC (Cooperação Econômica da Ásia e do Pacífico – Apec), com preferência ao uso na definição de dados “referidos” ou “relacionados” a pessoa. Ademais, observou a importância de relacionar a anonimização de dados ao conceito de razoabilidade. Representante do Intervozes salientou que a definição de consentimento, tal como apresentada no projeto de lei do Senado Federal (PLS 330/13), está melhor conceituada. Observou a diferença entre o consentimento forçado do livre e que aplicativos estão coletando dados excessivos sem opção para o usuário. Sublinhou que o consentimento deveria ser como o previsto no Marco Civil da Internet. Pesquisador do IDEC salientou a necessidade de constituição de autoridade independente e que precisa ser discutido como será a estruturação e o financiamento da agência, sugerindo que as multas poderiam ser repassadas para iniciativas de educação. Por fim, indicou que a regulamentação do setor não inibe as atividades, citando o exemplo do *Fair Credit Report Act* dos Estados Unidos.

Em 22/03/17 foi realizada Audiência Pública com a presença de representantes da Associação Nacional de Birôs de Crédito – ANBC, do Conselheiro do Comitê Gestor da Internet no Brasil - CGI.br, do Instituto Beta para Internet e Democracia – IBIDEM e da representante da Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público - Cedis/IDP-DF. A representante da ANBC defendeu que os dados biométricos não deveriam ser considerados dados sensíveis para fins de identificação ou conformação de identidade de pessoas naturais. Sugeriu também que o regramento de dados cadastrais deveria ser distinto dos de dados pessoais e que a *vacatio legis* da Lei fosse estendida a 36 meses. Arguiu, também, que o conceito de dados identificáveis fosse substituído para o de dados relativamente identificáveis, visto que, no limite do esforço computacional, quase todo dado é passível de identificação. O representante do IBIDEM defendeu, de modo geral, os termos do Projeto de Lei nº 5.276/2016 e apontou a necessidade de alteração do art. 13, de modo a não incluir o conceito de dado anonimizado no âmbito do conceito de dados pessoais. O representante CGI.br teceu algumas críticas à noção de interesse legítimo, alegando que a vagueza do conceito pode gerar problemas de interpretação e insegurança jurídica. Destacou, outrossim, que não se deve ter apenas um modelo de proteção de dados *ex ante*, sendo necessário que alguns temas sejam deixados ao controle *ex post*. Destacou, por fim, que não se deve permitir o condicionamento da prestação de serviços ao fornecimento de dados pelo usuário. Finalmente, a convidada do Cedis/IDP-DF, Laura Schertel, defendeu que não se pode excluir a inclusão da ideia de dados identificáveis e que a efetividade da proteção dos dados pessoais requer regulação *ex ante*, já que não se deve esperar a violação do direito acontecer para que o Poder Público aja. Ressaltou, ao fim, a conveniência de uma lei que abarque todos os setores, evitando a fragmentação que existe em países como os Estados Unidos, por exemplo.

Em 29/03/17 foi realizada Audiência Pública sobre o tema "Consentimento: Tratamento de Dados Sensíveis, Comercialização de Dados e Marketing Direto", com a presença de representantes da Associação Brasileira de Marketing Direto - ABEMD, do Instituto de Tecnologia & Sociedade do Rio – ITS e do Coordenador Institucional da PROTESTE. O representante da ABEMD destacou a necessidade de equilíbrio entre as empresas privadas e o Estado nas questões no tratamento de dados. Sugeriu a retirada do § 2º do art. 11 do PL nº 5.276/2016, que contém determinação expressa no sentido da não

realização de tratamento de dados “em detrimento do titular”. Explicou que a expressão “em detrimento” é por demais vaga, o que gera grande insegurança jurídica. O que exatamente configuraria, por exemplo, esse detrimento? Apontou a pertinência de uma *vacatio legis* maior, de pelo menos 3 anos e defendeu que os dados pessoais devem se referir a pessoas identificadas e não a pessoas identificáveis. Alegou que o conceito de “pessoa identificável” seria muito genérico e, no final das contas, com algum esforço, quase todos poderiam ser identificados, ou seja, quase todos são identificáveis. O representante da Proteste enfatizou que deve haver uma divisão de benefícios entre as empresas que se beneficiam desse novo mercado de dados e a população em geral. Defendeu, também, que que o órgão responsável deveria ser uma agência reguladora, com independência financeira e autonomia administrativa. Por fim, o representante do ITS teceu considerações sobre as discrepâncias entre as disposições do Marco Civil da Internet e as dos projetos em exame, no que refere ao tratamento dos dados pessoais. Mostrou que o Marco Civil traz, por exemplo, a necessidade de que o consentimento seja expresso, o que só ocorre para os dados sensíveis no âmbito do PL 5.276/2016. Arguiu que a nova lei de dados pessoais seria o local ideal para harmonizar o tratamento de dados.

Em 05/04/2017 foi realizada Audiência Pública sobre o tema "Legítimo Interesse”, com a presença de representantes da Federação Brasileira de Bancos - FEBRABAN, do Instituto Brasileiro de Direito Digital – IBDDIG, da organização não-governamental "Artigo 19" e de especialista em privacidade e proteção de dados e professor de Direito Digital e Internacional da Universidade Presbiteriana Mackenzie. O representante da FEBRABAN fez referência ao art. 29 da Data Protection Working Party para enfatizar que o conceito de legítimo interesse deve ser suficientemente claro e correspondente às atividades atuais ou benefícios almejados no presente pelo controlador, e feito por meio de um teste de equilíbrio entre os direitos fundamentais e os direitos do responsável em fazer o tratamento de dados. Indicou, ainda, que cada atividade possui um “legítimo interesse” diferente e que não seria possível, em razão disso, desenvolver uma definição fechada do conceito. Por fim, destacou que os direitos do responsável devem prevalecer sobre os do titular em casos de liberdade de expressão, fraude, lavagem de dinheiro, segurança de TI, monitoramento de empregados ou hipóteses semelhantes. A FEBRABAN sugere inclusão de novo inciso ao art. 16, do PL nº 5.276/2016, para possibilitar que a conservação dos dados pessoais após o término do

tratamento nos casos de legítimo interesse e para o cumprimento de obrigações legais ou regulatórias dos responsáveis. Sugere também que seja aditado o art. 18, VI, do mesmo projeto de lei, com o intuito de excetuar o direito de o titular dos pessoais solicitar a eliminação de seus dados pessoais, nas hipóteses de legítimo interesse. Em seguida, o presidente do IBDDIG criticou o modelo que impõe a necessidade de consentimentos repetidos, alegando que a consequência é uma “fadiga do consentimento”, o que conduz os titulares dos dados a um estado de impaciência, induzindo-os a consentir sem prévia reflexão. Defendeu que o mero consentimento não pode ser considerado uma panaceia. Explicou que o legítimo interesse protege de fato o usuário, pois não se limita ao consentimento expresso, o que, na prática, nunca protege o titular. A representante do Artigo 19 salientou que a incidência do legítimo interesse não deve impedir o direito ao esquecimento. Defendeu que o legítimo interesse só deve ser permitido dentro do que chamou de “expectativa contextual de privacidade”. Fotos de viagens, por exemplo, não poderiam ser utilizadas pela Receita Federal pois, nesse caso, não haveria legítimo interesse. Ou seja, deve haver correlação próxima entre a finalidade da aplicação e o tipo dos dados coletados. O professor da Universidade Presbiteriana Mackenzie explicou que o legítimo interesse é uma fuga da premissa de que o fundamento do tratamento de dados é sempre o consentimento. Alertou que o legítimo interesse não pode ser utilizado para justificar qualquer tipo de tratamento. Salientou, por fim, que o legítimo interesse deve ter fundamento num fato real, atual e não meramente especulativo a ser esclarecidos no futuro.

A Audiência Pública de 03/05/17 focou no tema “Responsabilidade Objetiva e Solidária”. Rafael Zanatta representando o IDEC (Instituto Brasileiro de Defesa do Consumidor) salientou a hipossuficiência do usuário na atividade de risco que representa a coleta de dados. Defendeu a responsabilidade objetiva e solidária, conforme o caso. Leonardo Bessa, diretor do BRASILCON (Instituto Brasileiro de Política e Direito do Consumidor) também defendeu esse tipo de responsabilidade e salientou que o Código Civil, arts. 159 e 927, garante que atividades que impliquem em risco devem ser enquadradas como de responsabilidade objetiva. Sugeriu, também, incluir no art. 42 do PL a expressão “independente de culpa”. Por fim, Leandro Alvarenga da CNDL (Confederação Nacional de Dirigentes Lojistas) defendeu que a responsabilidade do agente de tratamento deveria ser subjetiva e não envolver toda a cadeia, sob pena de engessar a economia e prejudicar, principalmente,

os pequenos empresários.

Em 31/05/2017 a AP tratou do órgão competente. Beatriz Kira, do Internetlab, salientou o consenso sobre órgão regulador autônomo com amplos poderes, financiado por taxas do setor (como no Reino Unido), dirigentes com mandato fixo, indicações por notório saber (Canadá) e sabatinados. Sobre autorregulamentação ponderou que deveria utilizada apenas de forma complementar. Cintia Lima, da USP/RP, indicou o caso italiano, a Autorita Garanti, composta de parlamentares, como um modelo sujeito a críticas pela não participação da sociedade. Discorreu sobre "o capitalismo informacional e a monetização dos dados pessoais" e a necessidade de se regular esse mercado relevante. Sugeriu que um órgão independente e autônomo desafogaria o judiciário e recomendou sua criação seguindo um modelo multissetorial, nos moldes do CGI, apesar de alegada crise. Alexandre Castro, do Sinditelebrasil, versou pela necessidade de uma legislação principiológica e equilibrada onde "a liberdade deverá ser a regra". Preconizou uma regulação *ex post* e alertou para "indústria da multa". Apoia a criação de órgão nos moldes de agência reguladora e que seu custeio não decorresse de taxas ou oneração dos agentes. Ulysses Machado, do Serpro, salientou que a regulação incluir o direito ao esquecimento, a obrigação da segurança da informação aos agentes de tratamento, a garantia do acesso dos órgãos de investigação aos dados cadastrais, estar em sintonia com a Política Nacional de Segurança da Informação e com a nova Lei de Identificação Civil. Lembrou que a autorregulação também pode ser invasiva e aumentar a judicialização, portanto melhor seria a criação de uma agência "*sui gêneris*" onde os diretores sejam eleitos com mandato. Gabriel Carvalho, do Depto. de Proteção do Consumidor, do MJ, é favorável à criação de órgão representante da sociedade, com capacidade de fiscalização e investigação, mas que também deve ser instituída uma Política Nacional de Proteção de Dados Pessoais e Privacidade. Ponderou que uma agência reguladora, com diferenças, ao contrário de autorregulamentação, seria a solução mais adequada. Maximiliano Martinhão, do SePin/MCTIC, informou que o órgão está elaborando uma estratégia para a economia digital, onde a internet das coisas tem papel fundamental e que essa modalidade de uso da internet demanda por alteração no regime de consentimento. Indicou que a agência deveria ser federal e com atuação mista entre regulação tradicional e corregulação, em conjunto com a indústria e a sociedade. Indicou que autorregulação seria frágil para esse mercado.

Em 07/06/17 a Audiência Pública tratou da transferência

internacional de dados. Bruno Magrani, do Facebook, ressaltou que os mecanismos de transferência devem incluir mecanismos de transferências entre empresas distintas e citou o Canada que permite a transferência de responsabilidade entre empresas. Danilo Doneda, da Open Knowledge Foundation, salientou que o Brasil poderia perder investimentos caso o "outsourcing" de dados não fosse permitido. Joana Varon, da Coding Rights, salientou a necessidade do “consentimento forte” e de autoridade para remediar e sancionar. Alertou para a perda de liberdade e o monopólio na internet na forma de “colonialismo digital”, salientando, como exemplos, a força dos *data brokers* (empresas que comercializam dados pessoais), ações do Google para permitir a cobrança no uso de bloqueadores de propagandas e do Facebook, que se utiliza dos microfones dos telefones de seus usuários. Thiago Sombra, da UnB, ressaltou não ser mais possível precisar por onde trafegam as informações e o papel dos intermediários, o que dificulta a imputação. Apontou a incongruência entre ser signatário do CISG[19], aliado do comércio internacional pela internet, e ter uma Lei de Acesso à Informação e não ter uma lei de proteção de dados. Instou pelo estímulo à autorregulação e corregulação e recomendou sistematizar em uma única seção a questão da responsabilidade e verificar sua compatibilidade com o disposto no Código Civil (Art. 927). Por fim ponderou acerca da exclusão da aplicação da lei para casos de transferência internacional para empresas em pais não certificado.

Em 05/07/2017 a Audiência Pública versou sobre o tema "Liberdade de Expressão e Proteção de Dados Pessoais”, com a presença de representantes da Associação Brasileira de Rádio e Televisão – ABRATEL, da Associação Brasileira de Emissoras de Rádio e Televisão – ABERT, do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas - CTS/FGV, do Fórum Nacional pela Democratização da Comunicação - FNDC e do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP. A representante da Abratel discorreu sobre a importância da transparência nas regras que regem a proteção de dados pessoais, de modo a se evitar insegurança jurídica, bem como sobre a essencialidade na manutenção das hipóteses de exceções trazidas pelas propostas legislativas em tramitação em relação ao tratamento de dados pessoais. O representante da FGV explicou a tensão e complementariedade entre as regras de liberdade de expressão e o direito à privacidade, que já constam do Marco Civil da Internet. Indagou acerca do

[19] Convenção de Viena das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias (CISG), do qual o Brasil faz parte desde 2013.

significado da expressão “domínio público” contida no PL 5.276/2016, e quais seriam as formas de diferencia-la de “interesse público”. Mencionou o art. 86 do Regulamento 2016/679 da União Europeia, que trata de acesso a documentos oficiais, para sugerir a inclusão de algo semelhante na lei brasileira. Destacou, também, que deveria haver maior clareza sobre o que se considera atividade jornalística. A ABERT comparou a importância do PL de proteção de dados ao citado Marco e ressaltou que a exclusão de atividade jornalística do âmbito da lei brasileira é fundamental. Ressaltou o caráter primário do direito ao lazer, destacando o papel da radiodifusão na disseminação de entretenimento e informação, inclusive no âmbito da internet. Destacou que o Código de Defesa do Consumidor, prescreve a necessidade de harmonização entre a proteção de defesa do consumidor e o desenvolvimento econômico e tecnológico, como preconiza a ordem econômica constitucional. Por fim, argumentou que as sanções mais graves deveriam ser ponderadas em vista da proporcionalidade da falta, alertando para os riscos de multas excessivas e abusivas, com potencial de comprometer a própria atividade econômica relacionada a dados no país. O FNDC sublinhou a não hierarquização entre os direitos fundamentais da livre expressão e da privacidade e a importância da separação entre a noção de dados pessoais e sensíveis. Defendeu a manutenção do art. 4º do PL do Executivo, para se evitar o cerceamento da atividade jornalística em nome da proteção de dados. Argumentou pela não inclusão de regras que tratem do “direito ao esquecimento”, sob o risco de restrições ao direito de o público receber informações. Nessa linha, sustentou a inclusão de dispositivo que vede a solicitação de exclusão de informações que são manifestamente de interesse público. Em conclusão, o INEP recomendou a noção expressa deste instituto na futura de lei, de modo a se garantir que eventual acesso por terceiros aos dados pessoais de alunos tenham como condição a anonimização destes dados, bem como a finalidade de pesquisa histórica, científica, estatística, ou a produção de estudos, avaliações educacionais ou de políticas públicas.

Em 11/07/17 a Audiência Pública tratou do tema da Agricultura de Precisão - AP. Fabricio Juntolli (CBAP-MAPA), destacou que o PL se encontra em estudo por comissão no âmbito do Ministério da Agricultura. Salientou a necessidade de colaboração entre produtores nas pesquisas com os dados gerados pela AP. Defendeu a pulverização do controle entre órgãos competentes. Alexandre Pacheco Silva (FGV-SP), alertou que, de acordo com o projeto, aliando-se um mapa de produtividade do solo à identificação do dono

da terra, os dados passariam a se tornam pessoais, um entrave à inovação. Recomendou a diferença conceitual entre dados autogerados pelo solo e pelas máquinas e os adquiridos externamente de agentes públicos e privados. Ponderou que apenas os dados brutos, de propriedade do agricultor, é que poderiam ser portabilizados. Acrescentou que o legitimo interesse na agricultura é importante, resguardado o direito à informação sobre a finalidade da coleta, e que a agência reguladora deveria ter parâmetros distintos no assunto, de acordo com cada setor. Pedro Palatnik (Abrasem), apresentou dúvidas acerca da titularidade dos dados gerados na AP, por exemplo aqueles gerados por operadores das máquinas, áreas arrendadas, processamento distribuído (como blockchain) e nas imagens de satélite em que as áreas são monitoradas - por motivos lícitos - sem consentimento. Sinalizou que a definição atual de dados pessoais permite que dados do solo sejam considerados pessoais, um retrocesso ao agronegócio. Classificou como ameaças a criação de órgão com ingerência sobre empresas, a fadiga de consentimento, o desestímulo à inovação, as restrições às transferências internacionais e a falta de clareza na distinção entre dados públicos e pessoais. Ricardo Inamasu (Embrapa), enfocou na necessidade do acesso público e transparente dos dados da AP, por exemplo para o controle de pragas e doenças, assim como o compartilhamento de dados de produção e das cooperativas. Rogerio Avellar (CNA), salientou que a AP é responsável pelo crescimento diferenciado das *startups* ligadas ao agronegócio. Salientou que a discussão sobre o tratamento de dados e a titularidade destes são questões debatidas tanto nos EUA como no Brasil e indicou o Privacy and Security Principles for Farm Data, de 2016, que estabelece os princípios a serem seguidos pelo setor naquele país. Destacou que o acesso aos dados pode se refletir diretamente no mercado e preços das *commodities* e indicou que o mais importante para o setor deveria ser a confiança e a transparência no tratamento dos dados.

Em 12/07/2017 foi realizada Audiência Pública sobre o tema "Inovação e Indústria 4.0”. O diretor da AMCHAM destacou que a legislação sobre proteção de dados tem impactos significativos na segurança jurídica de novos investimentos. Criticou os critérios da territorialidade contidos no PL 5.276/2016, alegando sua abrangência excessiva, e que os dados que apenas transitam no território nacional, e não pertencem a brasileiros, não deveriam estar incluídos na lei. Na mesma linha, argumentou que códigos de conduta e acordos de cooperação internacional deveriam possibilitar a

transferência internacional de dados. Defendeu que somente deveria ser considerado como dado pessoal aquele que realmente identifique o titular. Por fim, sustentou que a *vacatio legis* deveria ser condicionada à criação do órgão responsável, sem o qual a novel legislação não poderia ser devidamente aplicada. Em seguida, o presidente da ABES afirmou que a nova lei deveria possuir viés mais educacional que sancionatório, pois muitos dos problemas adviriam de falhas e falta de conhecimento dos próprios usuários dos serviços. Constatou a tensão existente entre a obrigação de transparência e a efetiva segurança dos dados, ressaltando a necessidade de fino equilíbrio da futura lei nesse ponto. Na sequência, o Gerente Executivo da CNI ponderou que uma legislação fraca e pouco detalhada gera insegurança jurídica, mas, por outro lado, uma regra demasiadamente minudente criaria desestímulos ao investimento. A CNI também apontou para as dificuldades do modelo atual de incidência das taxas de fiscalização (Fistel) nas comunicações máquina-a-máquina, o que poria em risco o desenvolvimento do mercado de Internet das Coisas - IoT. Ao fim, o representante da ABINEE, argumentou que a definição de dados pessoais é muito ampla e pode gerar confusão. Sugeriu que dado pessoal fosse somente aquele que, de fato, identifica o titular, excluindo a noção de "identificável". Aduziu, também, que a noção de anonimização deveria ser relativizada, já que a combinação de várias informações sempre, ou quase sempre, levará à identificação do titular dos dados, o que esvaziaria o significado de anonimização para efeitos de lei.

4. Seminário Internacional de Proteção de Dados Pessoais – 10 e 11 de Maio de 2017

No primeiro dia de Seminário, a primeira palestra foi da senhora Kara Sutton, da US Chamber`s Center for Global Regulatory Cooperation – GRC, que informou que o arcabouço dos EUA traz um forte caráter de auto-reglação e de autonomia e responsabilidade do usuário. Em sua opinião, a lei deve deixar espaço e priorizar a possibilidade de inovações, contendo definições claras, que tragam segurança jurídica. Alterações regulatórias constantes geram muita instabilidade. Em relação ao órgão competente, a senhora Sutton sugere que deve contar com jurisdição bem definida, ter

autonomia e que seus membros tenham estabilidade e sejam escolhidos mediante processo em que haja participação plural das instituições.

Em seguida, a senhora Piedade Costa de Oliveira, integrante do departamento Jurídico da Comissão Europeia, fez detalhado histórico da legislação de proteção de dados no âmbito da União Europeia, destacando que a era do Big Data exige também uma regulação que esteja à altura do desafio, como a Regulação 679/2016. Mencionou que o objetivo de uma lei geral de proteção de dados pessoais deve ser lidar de forma dinâmica com as novas tecnologias e acabar com a fragmentação regulatória. Ao final, salientou que a finalidade da Lei Geral de Proteção de Dados na Europa é facilitar a criação do mercado único digital na União Europeia, colocar nas mãos dos indivíduos o controle sobre seus próprios dados e aperfeiçoar a governança do modelo de proteção de dados pessoais.

Na sequência, a senhora Alejandra Andrea Vallejos Morales, assessora do Vice-ministro da Economia do Chile, reconstituiu os passos da história chilena na legislação da proteção de dados pessoais, que passou por vários modelos, desde os mais desregulamentados aos mais interventivos. Esclareceu que que o Chile já possui duas leis aprovadas e uma terceira em gestação. Explicou que o Chile desenvolveu ferramentas de *compliance* para maior efetividade na proteção de dados pessoais, enfatizando também a conveniência de a regulação criar incentivos positivos aos atores do mercado. Informou, também, que o orçamento do órgão competente para fiscalização das atividades de tratamento de dados no Chile seria baixo, da ordem de U$ 2 milhões anuais.

O Sr. Andrew Flavin, integrante do departamento de Comércio norte-americano, destacou o modelo setorial e fragmentado da regulação de proteção de dados nos Estados Unidos que, apesar de focar muitas vezes na auto-regulamentação, não deixa de ter um peso regulatório significativo. Em seguida, elaborou histórico do modelo americano da proteção de dados, desde o Privacy Protection Act de 1980 até os dias atuais e detalhou os trabalhos e a competência da APEC (Cooperação Econômica da Ásia e Pacífico) na proteção de dados pessoais, com destaque para a facilitação da interoperabilidade de modelos de proteção de dados pessoais de diferentes países, o que é essencial para livre circulação de bens e serviços num mundo globalizado.

A seguir, foi a vez da palestra da Sra. Joann Catherine Stonier, membro da Associação Internacional de Profissionais Defensores da Privacidade e da Mastercard. Stonier salientou que a lei de proteção de dados pessoais deve entender a conectividade dos ecossistemas que pretende regular, como no caso dos mercados de cartões de crédito. Como este mercado se utiliza de procedimentos em que não há relação direta com o consumidor, o procedimento padrão de obtenção de consentimento pode não se adequar plenamente. Destacou que o princípio da transparência, apesar de ninguém dele discordar em tese, não pode se transformar numa ferramenta que facilite fraudes. Explicou que a Lei europeia vislumbrou essas sutilezas. Por fim, apontou que a instituição do “legítimo interesse” é fundamental para uma regulação contextual de dados pessoais, e que os dados biométricos quando utilizados como mero recurso de identificação, não deveriam ser considerados dados sensíveis.

Depois falou o Sr. Alessandro Spina, do Centro de Proteção de Dados da Agência Europeia de Saúde. Spina declarou que na Lei Geral de Proteção de Dados da Europa a definição de dados de saúde é bastante abrangente, incluindo quaisquer serviços de saúde ou dados que, mesmo indiretamente, revelem informações de saúde. Na sequência, deixou claro que o setor de saúde é bastante peculiar, e que deve haver exceções às regras de consentimento que incluam, por exemplo, pandemias, ou questões específicas de cunho imigratório. Esclareceu, outrossim, que os conceitos de anonimização e pseudo-anonimização são muitos importantes para o tratamento de dados na área de saúde, levando a União Europeia e desenvolver métodos e técnicas bastante detalhados para anonimizar de forma mais eficiente os dados relativos à saúde.

Em seguida proferiu apresentação o Sr. Carlos María López, presidente global de assuntos regulatórios do grupo Telefónica. O palestrante iniciou enfatizando que estamos a viver uma era de disrupção inovadora não em razão da tecnologia, mas sim pelo grau de conectividade e pela ubiquidade de acesso à informação. Sublinhou a importância da transparência, do consentimento e do interesse legítimo na construção de uma lei isonômica para os vários atores e que possibilite a prestação de serviços específicos para diferentes usuários: os “introvertidos” e “extrovertidos”. No final, destacou que o setor de telecomunicações deseja também ter seu próprio espaço de dados e quer fazer parte do mercado de tratamento de dados

pessoais. O objetivo não é competir com grandes sítios da internet, mas para poder prestar melhores serviços a seus clientes.

O segundo dia teve início com a palestra da Sra. Leticia Lewis, da Software Alliance, que salientou a grande produção de dados e a consequente geração de empregos no tratamento de dados (para cada 1 emprego direto, há 3 indiretos). Explicou que é fundamental a necessidade da garantia da confiança, liberdade (entre fronteiras – considerando a ubiquidade e o processamento em nuvem), cooperação público-privado e, capacitação das pessoas.

Falou na sequência ao Sra. Natasha Jackson, da GSMA. Jackson informou que os dados constituem ativo fundamental muito mais importante que o petróleo porque estes não acabarem, serem reutilizados e adicionarem valor no seu processamento. Para Jackson, regimes restritos impedem a inovação e uma regulação inteligente deve ter as seguintes 5 características: baseada em princípios, com burocracia reduzida; apresentar baixo risco para o consumidor, evitando consentimentos desnecessários que geram fadiga para o consumidor; tecnologicamente neutra; leve, facilitando a transferência internacional, e; favorável ao investimento e à inovação, com ambiente de investimentos compatível com investimentos.

Por último, falou o Sr. John Miller, da Information Technology Industry, que salientou que os dados digitais geram um rastro considerável e, portanto, representam um perigo real para ataques virtuais, potencializado pela Internet das Coisas - IoT. Assim, há um aumento constante no risco para os cidadãos. A inteligência artificial representa um novo desafio pois dados são gerados por máquinas e a forma de lidar com isso ainda representa um desafio. Ressaltou que a lei deve prever diferentes tipos de consentimentos (contextualização), definição clara de dados sensíveis, balancear riscos com benefícios, notificação de quebras de segurança razoáveis, e uma regulação leve para a transferência internacional de dados.

5. Seminário Conjunto de Proteção de Dados Pessoais entre a Comissão de Ciência e Tecnologia, Comunicação e Informática e a Comissão Especial do PL 4060/12 – 22 de Maio de 2018

O Seminário foi aberto pelo Secretário de Políticas

Digitais do Ministro da Ciência, Tecnologia, Inovações e Comunicações, Sr. Thiago C. Lopes, que lembrou que o desafio na nova lei é proteger o usuário e ao mesmo tempo não barrar a inovação. O Secretário-Executivo do Ministério da Justiça, Sr. Gilson L. de O. Mendes, destacou que o tratamento de dados pelo setor público deve priorizar as ações de políticas públicas e a integração de seus sistemas. O Presidente da CCTCI, Dep. Goulart destacou a importância do debate para o futuro de oportunidades que se descortina.

A seguir foi realizado o painel “Abordagem regulatória para o tratamento de dados pessoais”. O Secretário do MCTIC, que participou da abertura, complementou seu posicionamento, mencionando a importância da Estratégia Brasileira de Economia Digital, que a criação de um ente deveria ser cotejada com o limite de gastos e que o excesso regulatório pode representar “exportação de oportunidades”. Luis F. S. Monteiro, Secretário de Tecnologia da Informação e Comunicação do MPOG, destacou a inciativa *gov-data*, útil para o cruzamento e checagem do grande volume de informações guardadas pelos órgãos públicos. Frederico M. Ceroy, Promotor de Justiça e Coordenador da Comissão de Proteção de Dados do MPDFT destacou que uma regulamentação detalhada é positiva e de que a autoridade deveria ser concentrada em uma única pessoa, rodeada de engenheiros e poliglotas. Ana Carolina P. C. Guimarães, Diretora do Departamento de Proteção e Defesa do Consumidor da Senacom/MJ, destacou a importância das autoridades de defesa do consumidor estarem inseridas no órgão regulador. Demi Getschko Diretor-Presidente do NIC.br destacou a característica multissetorial da atividade e que a regulação deve prever a dinâmica colaborativa. Ademais, ponderou que a aplicação dos dados deve ser transparente e ética, uma vez que a tendência é de que os dados vazem, em algum momento. Bruno Gencarelli, representante da DG Justiça e Consumidores da União Europeia, destacou que a regulamentação deve ser adaptativa à tecnologia e que o Brasil é um importante ator no fluxo internacional de dados. Márcio Barreto membro da ABC, Cidacs e Fiocruz, destacou que a pesquisa com dados sensíveis e a agregação de dados oriundos de amostras massivas gera oportunidade de construção de políticas públicas.

O segundo painel tratou de “O uso de dados pessoais como instrumento de campanha eleitoral e a persuasão da opinião pública". André Torretta, da A Ponte Estratégia, explicou a segmentação de personalidades para fins de propaganda eleitoral. Nathalie Gazzaneo,

representante do Facebook, esclareceu que a plataforma não vende dados pessoais, que está trabalhando sua transparência e que no episódio da Cambridgy Analytica, 443 mil brasileiros foram atingidos e que 200 aplicativos estão sendo revisados. Bruna Santos, representante da Coalização Direitos na Rede, defendeu a transparência na publicidade e o combate ao discurso de ódio. Paulo M. R. Brnacher, da PUC/SP, destacou a dificuldade das plataformas serem neutras e que a educação do eleitor deve ser reforçada para que este melhor reflita sobre táticas de convencimento. Gustavo Artese, da associação IAPP, destacou a fadiga do consentimento e de que a lei deve ser principiológica.

O último painel abordou "Tratamento a notícias falsas - *fake news*". Natalia Viana, Codiretora da Agência Pública, destacou que os "fact-checkers" são uma tendência em crescimento e que há um processo de certificação internacional. Carlos A. de Moraes Afonso, afirmou que os "fact-checkers" omitem conteúdos e são parciais. Marcelo Lacerda, representante do Google, prefere o uso do termo "desinformação" e ressaltou a importância do jornalismo e da educação dos usuários. Fábio Gouveia, do Labic da UFES, explicou o apelo desse tipo de notícias e asseverou que o jornalismo precisa se adaptar a enfrentar as "bolhas ideológicas". Jonas Valente, do Intervozes, lamentou o uso de dados pessoais para espalhar a desinformação, mas manifestou ser contrário à criminalização. Márcio S. Novaes, da Abratel, defendeu a responsabilização dos grandes grupos da internet e a necessidade de fortalecimento da educação. Marcelo Bechara, da Abert, lembrou dos "deep-fakes", muito mais verossímeis, como a desinformação prejudica a democracia e também defendeu alguma forma de se responsabilizar as empresas da internet.

6. Contribuições Recebidas

Ressalte-se que esta relatoria recebeu 20 contribuições ao texto oriundas de diversos setores. As propostas se encontram devidamente disponibilizadas na página da internet desta Comissão Especial.[20] Além disso,

[20] Sítio internet da Comissão Especial; http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais, acessado em 03/04/18.

esta relatoria tomou conhecimento de Nota Técnica nº 04/2016/SCI/PGR,[21] do Ministério Público Federal, em que são oferecidas sugestões de aperfeiçoamento ao texto do PL nº 5.276/16.

A importância do tema também é enfatizada pelo Tribunal de Contas da União. A corte encaminhou oficialmente cópia do Acordão TC-034.896/2015-5, da relatoria do Ministro Benjamin Zymler, que trata de auditoria operacional realizada com objetivo de avaliar a condução da política de abertura de dados da administração pública. Em suas conclusões a auditoria conclui por:

> *"79. Ademais, a inexistência de legislação que especifique claramente o que são dados pessoais e como eles devem ser tratados pelo Poder Público pode causar insegurança nos gestores para enquadrar como pessoal uma informação pertencente as suas bases de dados, gerando riscos tanto de restrição a dados que deveriam estar disponíveis publicamente quanto de divulgação inadvertida de dados pessoais."*

Verifica-se assim, que o egrégio tribunal constata ser imperativa para a consecução de políticas públicas concernentes ao setor de TIC um marco regulatório que permita proteger os dados das pessoas.

7. Nosso Encaminhamento

Vivemos um mundo novo em que as TIC (Tecnologias da Informação e das Comunicações) possibilitaram uma transformação no modo de viver e abriu outra dimensão na oferta de produtos e serviços. Há quem proponha que vivemos na era da Revolução Industrial 2.0, na Era Digital, da Convergência Digital, na Era dos Dados. As novas tecnologias e o conhecimento dela gerado possibilitou o aumento no acesso a serviços básicos e essenciais, assim como a proliferação de ofertas para tornar a vida melhor. O insumo vital nesse cenário que se descortina é o tratamento dos dados gerados pelos usuários: a descoberta de padrões, casualidades, predição e agregação de valores, tendências e adaptação de resultados, são algumas das ferramentas utilizadas. As aplicações do conhecimento gerado do tratamento de dados são infindáveis e, certamente, inimagináveis aos olhos de hoje.

---

[21] Íntegra da Nota Técnica disponível em: http://www.mpf.mp.br/pgr/documentos/NotaTcnica04_2016proteodedados.pdf, acessado em 21/07/16.

Também não há como desconhecer que vivemos em uma era em que grandes corporações do setor de TIC, assim como governos, possuem e adquirem, diariamente, imensas quantidades de dados acerca de seus usuários, assinantes, consumidores e cidadãos. Tampouco que o tratamento de dados pessoais, sem as devidas salvaguardas, pode violar a privacidade e a intimidade das pessoas, assim como afrontar os mais variados direitos humanos e o princípio democrático.

O conhecimento de marcadores genéticos pode ajudar no desenvolvimento da medicina, mas a informação também poderia ser manipulada para encarecer ou alijar pessoas do acesso ao trabalho, a planos de saúde ou outros serviços. Dados locacionais adquiridos por aplicativos de trânsito podem ser repassados para seguradoras para traçar o perfil de motoristas e permitir a oferta de produtos mais baratos, mas também poderiam ser utilizados para negar cobertura a moradores de determinadas ruas ou regiões. Grupos organizados podem fazer ecoar suas mensagens com maior força junto ao seu público alvo, mas também poderiam realizar ações de "guerra política" nas redes sociais, se valendo das informações prestadas inadvertidamente pelos usuários. Redes de comércio varejista, autoridades de segurança pública, partidos políticos e as mais diversas associações podem igualmente estar recebendo diversos dados do perfil de internautas, usuários de telefonia ou telespectadores, e tomando decisões que afetam diretamente as vidas dessas pessoas. Em tempos em que cada pessoa possui um rastro digital praticamente impossível de ser apagado, é certo que o uso indevido ou o vazamento dessas informações poderá causar danos irreparáveis aos indivíduos e à coletividade.

Por outro lado, ao se viver nesta era em que dados e informações se tornaram insumos de negócios e movimentam vigorosíssimas indústrias globais, é extremamente necessário tornar o Brasil um ambiente integrado com o mundo e, portanto, propício para o desenvolvimento do setor. Por esse motivo e como discutido anteriormente, a não proteção aos dados pessoais, pode alijar o país de importantes oportunidades de desenvolvimento econômico.

Devido a esses dois aspectos, o da necessidade da promoção da proteção da pessoa humana e o do desenvolvimento e da integração do setor de TIC como ferramenta de desenvolvimento econômico para o País, **somos, no mérito, pela aprovação das matérias**.

Entretanto, o estudo criterioso dos projetos, a análise ponderada das contribuições recebidas e das Emendas apresentadas em Plenário e o cotejamento destes materiais com os comentários registrados nas audiências e seminários conduzidos nesta Comissão Especial, nos levam à conclusão de que diversos melhoramentos podem ser apresentados aos textos em análise por esta Comissão Especial.

Por essas razões, submeto um **SUBSTITUTIVO** às proposições. Passamos agora a explicar ponto a ponto as alterações sugeridas. Esclarecendo que alterações menores de redação a dispositivos existentes nos projetos ou de cunho de técnica legislativa não serão aqui relatadas.

8. As Principais Modificação Introduzidas pelo Substitutivo

[Art. 2º] – Direitos Humanos

Entendemos que os direitos humanos, o desenvolvimento da personalidade e dignidade e o exercício da cidadania são diretamente afetados pelo tratamento de dados pessoais realizados pelos diversos setores, com consequências em variados aspectos da vida em sociedade. Portanto, incluímos entre os fundamentos da disciplina da proteção de dados, o **inciso VI no art. 2º**, nesse sentido.

[Art. 4º] – Do tratamento de dados de segurança pública

Devido à importância da matéria, prevemos que os dados de **segurança pública e nacional** devem ser regidos por legislação específica, entretanto, assim como nas legislações de outros países, a norma geral de proteção de dados deve nortear determinados princípios quanto às relações entre os agentes envolvidos no tratamento. Por esse motivo, incluímos a determinação, no **§1º do Art. 4º**, de que Lei específica deverá prever o atendimento do interesse público para esse tipo de tratamento. Ademais, devido à natureza crítica para a soberania e segurança das pessoas e das

instituições adicionamos o **§4º** ao mesmo artigo determinando, inspirados no art. 10º da nova Resolução europeia, que, para esse tipo de dados pessoais, os bancos de dados **não podem ser totalmente objeto de terceirização** junto ao setor privado.

[Art. 5º] – Definições da Lei

A definição de **dados sensíveis** é fortemente inspirada naquela contida no projeto de Lei apresentado pelo Dep. Milton Monti. Nesse particular, esses dados, como o nome sugere, demandam camada adicional de proteção. Nesse sentido, o projeto prevê, assim como no projeto do autor da matéria principal, que o seu uso deverá ser precedido da obtenção de um consentimento por parte do titular dos dados. No nosso caso, optamos por prever um consentimento **específico e em destaque**. Entretanto, percebemos que são sensíveis apenas aqueles relacionados a pessoas naturais. Assim, dados genéticos oriundos de plantas - de interesse do agronegócio ou da chamada agricultura de precisão, por exemplo - ou anonimizados deixam de ser sensíveis. Por esse motivo alteramos a definição de dados sensíveis, no **inciso II do art. 5º**, incluindo o condicionante de que serão assim considerados somente quando vinculados a uma pessoa natural.

É fato que o desenvolvimento do poder computacional é crescente e contínuo. Dessa forma a **anonimização de dados** de hoje pode se tornar obsoleta amanhã. Ademais, apesar de um responsável utilizar técnicas apropriadas de anonimização e de segurança, a adição de outros dados, oriundos de outro provedor, ou novas tecnologias poderão permitir a identificação de titulares. Por isso, é razoável admitir que a anonimização absoluta e a prova de falhas é impossível de ser atingida e garantida a qualquer tempo. Em outras palavras a anonimização é passível de ser revertida em determinadas situações. Por esses motivos, incluímos uma relativização temporal e tecnológica nas definições constantes nos **incisos III e XI**, determinando que os dados serão considerados anonimizados quando utilizadas técnicas razoáveis e disponíveis à época de seu tratamento.

Como forma de dar maior clareza aos comandos gerais optamos por incluir definições para “**relatório de impacto** à proteção de dados pessoais”

(inciso **XVII**), "**órgão de pesquisa**" (**XVIII**) e "**órgão competente**" (**XIX**). Para o primeiro determinamos que o relatório deverá conter a documentação dos processos que possam gerar risco, bem como as medidas de mitigação. Os órgãos de pesquisa são aqueles consagrados pela legislação de ciência, tecnologia e inovação, isto é, órgãos públicos ou privados sem fins lucrativos, que possuam como missão institucional a pesquisa básica ou aplicada. Por fim, uma vez que o projeto encaminhado pelo Poder Executivo determina a designação de um órgão responsável sem, no entanto, o especificar, definimos que essa instituição fará parte da administração pública indireta, é será a responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

[Art. 7º] – Hipóteses de tratamento

Cotejando os Projetos de Lei em análise propomos dez hipóteses para o tratamento de dados pessoais, sendo, a principal delas, mediante a obtenção de consentimento livre, informado e inequívoco. Prevemos o tratamento no cumprimento de obrigação legal, regulatória, contratual, estudos, processos judiciais, entre outros. Ademais, julgamos pertinente incluir (**inciso X**) recepção expressa à possibilidade de abertura de cadastro de consumidores para proteção do crédito, tal como consagrada no art. 43 do Código de Defesa do Consumidor.

Devido à popularidade e ubiquidade das novas mídias digitais, percebemos que há casos em que o próprio titular torna parte de seus **dados manifestamente públicos**. Para esses casos, incluímos um novo **§4º**, em que fica dispensada a obtenção do consentimento, resguardados os direitos do titular e demais princípios desta Lei, por exemplo, a solicitação de exclusão de dados ou suspensão do tratamento.

A profusão de aplicações para os dados pessoais, assim como de empresas do mesmo e de outros grupos empresariais que realizam o **compartilhamento de dados coletados de titulares**, evidenciou, em vários casos, a perda do controle do titular sobre seus próprios dados. Como forma de permitir um maior domínio, assim como facilitar a revogação de consentimentos porventura concedidos, prevemos um novo **§5º**, dispondo que na transferência de dados para outros responsáveis será necessária a obtenção de consentimento específico para esse fim. Ressalte-se que essa

autorização pode ser obtida ao mesmo tempo em que se obtêm os demais consentimentos. Apenas deverá ser destacado dos demais.

[Art. 9º] – Direito a informações sobre o tratamento

Sem controles de consentimentos, os dados, nos meios digitais, podem ser repassados indefinidamente entre responsáveis, o que enseja redução da possibilidade do exercício de alguns dos direitos pelos titulares. Para garantir a eficácia das garantias dadas ao usuário, incluímos a sugestão, contida no **inciso V do art. 9º**, de que somente será necessário comunicar o titular em casos em que os dados forem efetivamente **compartilhados com terceiros responsáveis**, quando devidamente consentido. Assim diminui-se a necessidade de consentimentos constantes. Em comlemento, também optamos por incluir uma camada adicional de proteção, mediante a inclusão do **§ 2º**, para que o titular seja informado a cada vez que surgirem **novas finalidades** para o tratamento dos dados.

[Art. 10] – Legítimo Interesse

O legítimo interesse representa uma das hipóteses de tratamento de dados pessoais sem a necessidade de prévia obtenção do consentimento e sua introdução na proposta é inspirada nas práticas europeias existentes desde 1995.

Sua previsão é necessária, seja para não onerar demasiadamente o titular dos dados com a necessidade de manifestação de consentimento a todo instante, seja porque em diversas situações concretas o tratamento de dados, mesmo sem consentimento, é importante para atender a uma finalidade pública ou a uma finalidade privada legítima, tal como a prevenção a fraudes bancárias ou a garantia de segurança das redes.

O legítimo interesse, contudo, não deve ser lido como um cheque em branco. Em outras palavras, não pode ser utilizado como um subterfúgio para que todo e qualquer tratamento de dados pessoais seja autorizado. Esta a razão dos parágrafos do artigo, mediante os quais se destaca que o legítimo interesse deve sempre vir acompanhado dos princípios da adequação, necessidade e transparência bem como da possibilidade de

fiscalização. Ademais, prevemos que deverá se basear em **situação concreta** e desde que atendidas as **legítimas expectativas do titular**.

[Art. 11] – Dados Sensíveis

Como há duas categorias de dados, os dados pessoais (“gerais”) e, nessa categoria, o subconjunto dos dados sensíveis, resolvemos por discriminar os tipos de **consentimentos**. Para a primeira categoria de dados, o consentimento é livre, informado e inequívoco. Já para a segunda categoria, explicitamos, no **art. 11**, que esse consentimento deverá ser **específico e em destaque para finalidades específicas**, adicionais às contidas no consentimento referente ao tratamento de dados pessoais “gerais”. Dessa maneira, a necessidade de se obter consentimento em destaque é, assim, a camada adicional de proteção para este tipo de dados. Todavia, tendo em vista a necessidade de **combater fraudes em processos de identificação**, incluímos nova alínea **“g”, ao inciso II**, que contêm as exceções à necessidade de obtenção de consentimento específico, excetuando da obrigação de obtenção de consentimento também para este caso.

[Art. 12] – Dados Anonimizados

Além de relativizar o conceito de anonimização dos dados no artigo das definições, levando em consideração a razoabilidade, optamos por incluir novo **§ 1º** para que sejam considerados **fatores objetivos**, tais como custo, tempo, tecnologias disponíveis no momento e a utilização exclusiva de meios próprios. Ademais, alteramos a redação do agora, **§ 2º** para considerar, como dados pessoais, aqueles utilizados para a formação do **perfil comportamental** de uma determinada pessoa natural apenas se a pessoa for identificada.

[Art. 13] – Dados de Saúde

Tendo em vista o enorme potencial dos dados referentes à saúde para o desenvolvimento de novos produtos e serviços, tais como novos tratamentos e drogas para doenças crônicas e degenerativas, e, ao mesmo tempo, o alto impacto que o seu tratamento pode gerar na vida e nos direitos fundamentais das pessoas, optamos por incluir um regramento balizador para o uso destes dados. O **art. 13**, determina que os órgãos de pesquisa, assim definidos nesta Lei, terão acesso a estes dados para a realização de **estudos em saúde pública**, desde que para uso exclusivo dentro dos órgãos, para a finalidade específica de pesquisa e quando mantidos em ambiente seguro. Ademais, os dados deverão ser anonimizados, sempre que possível, e os resultados obtidos não poderão revelar dados pessoais. Por outro lado, considerando a notável complexidade dos procedimentos, protocolos e códigos de conduta, a dispersão dos bancos de dados e a variedade de atores envolvidos com este tipo de tratamento, tanto públicos como privados, determinamos que tanto o órgão regulador, quanto as autoridades de saúde poderão emitir **regramentos específicos**, no âmbito de suas competências.

[Art. 14] – Crianças e Adolescentes

Na questão do tratamento de dados de crianças e adolescentes, o Projeto original apenas determina, de maneira superficial, que a atividade deva se dar “no seu melhor interesse, nos termos da legislação pertinente”. Entendemos que esse comando não acrescenta nenhuma proteção especial para esse vulnerável grupo de pessoas. Não é o que ocorre em outros países. Nos EUA, como já foi dito, o Children's Online Privacy Protection Act, de 1998, conhecida como Lei COPPA,[22] possui importante contribuição, a qual utilizamos como inspiração para a questão.

Decidimos incluir, como regra geral, ser ilegal a coleta de dados pessoais de crianças, abaixo de 12 anos de idade, sem o consentimento

[22] Disponível em http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5, acessado em 14/07/16.

específico e em destaque dado por pelo menos um dos pais ou responsável legal. Nesses casos, o responsável deve realizar todos os esforços razoáveis para verificar que esse consentimento foi dado efetivamente pelo responsável pela criança, levando em consideração as tecnologias disponíveis. A exceção é quando a coleta seja necessária para contatar os pais ou responsável legal.

Criamos também uma vedação para que os responsáveis condicionem a participação de crianças a jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais que excedam ao estritamente necessário para participar dessas atividades. Ademais, responsáveis que lidem com dados de crianças e adolescentes deverão manter pública informação sobre os tipos de dados coletados, como estes são utilizados e os procedimentos para o exercício dos direitos dos titulares.

Por fim, determinamos que as informações referentes ao tratamento dos dados referidos deverão ser fornecidas de maneira simples, clara e acessível, consideradas, dentre outras, as características intelectuais e mentais do usuário.

[Art. 15] – Do Término do Tratamento

Excluímos a previsão de que o órgão competente deverá estabelecer **períodos máximos para o tratamento**. Primeiro por se tratar de relação jurídica eminentemente privada, de trato sucessivo entre as partes e depois porque a própria proposta legislativa já contém mecanismos capazes de evitar eventuais abusos por parte dos responsáveis pelo tratamento dos dados, como o princípio da finalidade, adequação e necessidade. Ademais, como forma de evitar a possibilidade de exclusão de dados que sejam de interesse público, incluímos previsão nesse sentido no **inciso III**.

[Art. 18] – Dos Direitos do Titular

Os direitos dos titulares sobre os seus dados são o elemento essencial deste arcabouço. Nesse sentido, acrescentamos quatro novos direitos ao titular não previstos em nenhum dos projetos, a saber: informação das entidades públicas e privadas com as quais o responsável realizou **uso**

compartilhado de dados (inciso VII); informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de eventual **negativa de consentimento (VIII)**; a **revogação do consentimento** nos termos do § 5º do art. 8º **(IX)**, e o direito de peticionar junto ao responsável **(X)**. Com isso, os direitos do titular ficam robustecidos, já que este passa a dispor de meios e informações para proteger mais efetivamente seus dados pessoais.

Por fim, entendemos não fazer sentido o direito de portabilidade de dados anonimizados já tratados pelo responsável, e por isso excluímos tal possibilidade.

[Arts. 23 a 30] – Tratamento pelo poder público e Compatibilização com a Lei de Acesso à Informação

A LAI (Lei de Acesso à Informação, Lei nº 12.527/11) estabelece para toda a Administração uma série de procedimentos a serem observados com vistas a garantir o acesso pela população a informações por ela guardadas. Há requisitos para o tratamento de pedidos de acesso, de classificação do sigilo das informações e de proteção na guarda de dados pessoais. Ademais, um dos pilares da Lei estabelece que cada órgão deverá designar **autoridade responsável** pelo cumprimento das normas emanadas desse instrumento. Tendo em vista que a LAI representa importante avanço no trato das informações pelo Poder Público e que o seu atendimento está devidamente cristalizado na Administração, adequamos os artigos que tratam do "Tratamento de Dados Pessoais Pelo Poder Público" (**arts. 23 a 30**), de modo a prever a sistemática pormenorizada na LAI para o tratamento dessas informações no escopo desta Lei, bem como a continuidade da autoridade lá prevista.

Como forma de ampliar a proteção à privacidade das pessoas quando seus dados são tratados pelo poder público, incluímos dispositivo para proteger e preservar os dados pessoais de requerentes de acesso a informações públicas (**Art. 23, inciso II**). Ademais, como forma de aumentar a transparência do serviço público incluímos novo artigo (**Art. 25**), determinando que as informações deverão ser fornecidas em formatos interoperáveis que permitam o uso compartilhado e a disseminação de informações.

[Art. 33 a 36] – Transferência Internacional de Dados

Além dos países, consideramos como sujeito da transferência internacional de dados, no **inciso I do art. 33**, as organizações internacionais, pessoas jurídicas de direito internacional público. Dessa forma, serão possibilitadas e facilitadas as transferências de dados, fundamentais para o trabalho de tais entidades multilaterais. Ainda no referido inciso optamos pelo uso do conceito de "proteção adequada" ao invés de "proteção equiparável", com o intuito de deixar a ideia da comparação do grau de proteção mais restrita e menos ambígua.

Inserimos novo **inciso II ao art. 33** para incluir outras formas de reconhecimento de proteção de dados pessoais pelo órgão competente, tais como cláusulas contratuais específicas para uma determinada transferência, cláusulas contratuais padrão, normas corporativas globais, e a emissão de selos, certificados ou códigos de conduta e adequação, emitidos por organismos internacionais. Tal solução vem sendo adotada por vários países do mundo.

No inciso **VIII do art. 33** aditamos a obrigação de o consentimento ser específico e em destaque para a transferência internacional, em razão da importância que envolve esse tipo de transferência. Em seguida, acrescentamos **inciso IX ao art. 33** para permitir a transferência internacional, ainda que sem consentimento, nas hipóteses de cumprimento de obrigação legal ou regulatória pelo responsável, para a execução de um contrato ou de procedimentos preliminares de um contrato do qual é parte o titular, e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Inserimos **parágrafo único ao art. 33** para prever a possibilidade de pessoas jurídicas de direito público e responsáveis, sob determinadas condições, requererem ao órgão competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional.

O **art. 34** acrescenta a obrigação de se observar a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.

Na sequência, o **art. 35**, habilita o órgão competente a definir o conteúdo

de cláusulas contratuais padrão e proceder à verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais, selos, certificados e códigos de conduta. Previmos a possibilidade de o órgão competente requerer informações suplementares ou realizar diligências de verificação quanto às operações de tratamento, bem como o poder de designar organismos de certificação, que estarão sob sua fiscalização.

Finalmente, com o objetivo de assegurar a manutenção dos direitos dos titulares no âmbito da transferência internacional de dados, o **art. 36**, que dispõe que quaisquer alterações nas garantias apresentadas pelo responsável deverão ser comunicadas ao órgão competente.

[Art. 38] – Relatório de Impacto à Proteção de Dados

Entendemos que a elaboração de relatórios de impacto à proteção de dados é uma atividade benéfica no gerenciamento do negócio pelo próprio responsável. A elaboração permite uma reflexão sobre os procedimentos adotados e contribui para a identificação de eventuais falhas, mitigando a possibilidade de danos antes mesmo que estes ocorram. Assim, a elaboração prévia por motivações próprias é extremamente salutar para os agentes de tratamento. Entretanto, entendemos que esta deve ser uma decisão dos próprios agentes e não uma imposição da burocracia.

Com essa lógica em mente e considerando que o projeto prevê a elaboração de relatórios de impacto, sentimos a necessidade de detalhar os principais objetivos que devem ser cumpridos mediante a elaboração do referido documento (**art. 38**). Determinamos que o relatório deverá minimamente abordar a **descrição dos dados coletados, a metodologia de coleta e as medidas de segurança adotadas**. Ademais, o relatório deverá possuir a análise do responsável sobre os mecanismos adotados para a mitigação de riscos.

[Arts. 42 e 45] – Responsabilidade e Ressarcimento de Danos

A atividade de tratamento de dados pessoais constitui atividade de risco, o que atrai a incidência da responsabilidade objetiva ao agente de

tratamento, ou seja, aquela segundo a qual não há necessidade de perquirir a existência de culpa para obrigar o causador do dano a repará-lo. Esta já é a regra geral do direito brasileiro para toda e qualquer atividade de risco, conforme previsto no parágrafo único do art. 927 do Código Civil, como também constitui a base da responsabilização dos fornecedores nas relações de consumo.

Tendo ainda em vista que o tratamento de dados frequentemente envolve mais de um agente e como não deve ser do titular dos dados o ônus de descobrir dentro de uma cadeia econômica quem deu causa ao dano sofrido, o **§ 1° do art. 42** estipula a **responsabilidade solidária sempre que houver responsáveis atuando em conjunto,** bem como estabelece a responsabilidade solidária do operador quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável.

O **art. 43** prevê, à maneira do Código de Defesa do Consumidor - CDC, as **hipóteses de exceção à responsabilidade civil** do responsável e do operador. Também com o objetivo de garantir maior segurança jurídica aos agentes de tratamento, entendemos conveniente prever de forma expressa o **direito de regresso**, com a inclusão do **§ 4º ao art. 42.**

Ademais, o tratamento de dados é atividade típica das sociedades complexas e de massa da atualidade, sendo de bom alvitre assegurar instrumentos processuais voltados à garantia e defesa em juízo de direitos difusos, coletivos e individuais homogêneos **(art. 40, § 3°)**. Para a defesa em juízo, achamos também fundamental deixar clara a incidência da teoria dinâmica do ônus da prova, segundo a qual tal ônus deve recair sobre a parte que tiver maiores condições de dele se desincumbir, à vista da cooperação e da boa-fé processual **(art. 40, § 2°)**.

Atento ainda ao fato de que o tratamento de dados é atividade essencialmente dependente do avanço tecnológico de determinada época, o projeto de lei alerta, **nos artigos 43 e 44**, para a correlação existente entre a regularidade da atividade e o estado atual da tecnologia, a qual sempre impactará nos riscos envolvidos no tratamento e na segurança das redes.

Por fim, ciente de que o tratamento de dados pode alcançar tanto relações consumeristas como de outra natureza, a proposta pretende

determinar que a responsabilidade civil em casos a envolver o direito do consumidor continua inteiramente regida pelo CDC, que estabelece como um dos critérios da política nacional das relações de consumo a: " *[...] compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores*" **(CDC, art. 4°, inciso III).**

[Art. 46 ao 51] – Da Segurança e das Boas Práticas

O estabelecimento de regras de boas práticas e de governança são fundamentais para o bom desenvolvimento de qualquer ramo de atividade pública e empresarial. Por sua vez, a moderna regulação deve ser leve e flexível, estimulando o desenvolvimento livre, porém seguro, das atividades. Com esse espírito, entendemos que o órgão regulador deve estimular a autorregulamentação e a adoção de padrões de qualidade e de segurança, visando a mitigação de riscos no tratamento de dados pessoais. Esse caráter opcional e indutor é, por exemplo, a abordagem contida no Art. 40 da nova Regulação europeia, assim como o emanado do arcabouço dos EUA. Este inclusive é mais um grande mérito incorporado do projeto apresentado pelo Dep. Milton Monti.

Por esses motivos incluímos o **art. 49** que contempla rol de procedimentos próprios de um programa de **governança e de boas práticas, a ser implementado opcionalmente** pelo responsável pelo tratamento dos dados pessoais. O objetivo é proporcionar um conjunto de ações que minimizem o risco das atividades de tratamento e seus eventuais danos. Ademais, prevemos que a adoção desses procedimentos pode implicar **redução de eventual sanção** a ser aplicada, nos termos do **inciso VIII do § 1º do art. 52** da presente proposta. Por último neste particular, incluímos o **art. 51** atribuindo ao órgão competente a função de estimular a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados.

[Art. 52] – Sanções Administrativas

As alterações promovidas foram no sentido de incrementar o rol de sanções e melhor graduar a sua aplicação, melhor detalhando os elementos e circunstâncias para o estabelecimento das penalidades. Com esse desiderato, acrescentamos as penalidades de **advertência com prazo**, **eliminação** de dados pessoais, **suspensão** do exercício da atividade de tratamento de dados pessoais e **proibição** parcial ou total do exercício dessas atividades. Optamos pela supressão da penalidade de anonimização dos dados pessoais, visto constituir medida de proteção dos dados e não sanção.

Em relação à pena de multa, do modo como fazem outras legislações, estabelecemos parâmetros e limites para os valores de aplicação de multas. No caso brasileiro, verificamos que tanto a Lei Geral de Telecomunicações (Lei nº 9.472/1997) e a Lei de Sanções Penais e Administrativas Ambientais (Lei nº 9.605/1998), arbitraram, há mais de vinte anos, um teto de multas de R$ 50 milhões de reais. A Lei do Sistema Brasileiro da Concorrência (Lei nº 12.529/11) estabelece percentuais de multas de até 20% calculados sobre o valor do faturamento bruto anual do grupo. A Lei nº 13.506/17, do sistema financeiro, preceitua que as multas podem variar entre 0,5% da receita de serviços ou até 2 bilhões de reais. Mais próximo ao setor, o Marco Civil da Internet prevê multa de até 10% do faturamento do grupo no país para as penalidades que determina. No caso europeu a multa pode chegar a 10 milhões de Euros ou 2% do faturamento global.

Com base nessa comparação nacional e internacional, entendemos que a combinação entre um percentual e um valor absoluto da multa não é caso isolado e não é estranha ao ordenamento jurídico brasileiro, sendo perfeitamente razoável que a futura Lei Geral de Proteção de dados Pessoais assim disponha. Por esses motivos determinamos, **no inciso I do art. 52,** que a **multa** simples não poderá ultrapassar **4% do faturamento** da empresa, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, e deve ser **limitada a R$ 50.000.000,00** (cinquenta milhões de reais), por infração. Lembramos a necessidade de se incluir a menção expressa a grupos ou conglomerados, pois, à semelhança da citada Lei de Concorrência (o Cade da nova Lei nº 12.529/11), é importante prever a cobrança de multas de corporações, se existirem, em caso de impossibilidade de se atingir financeiramente a empresa que realizou a

infração.

No que se refere aos elementos circunstanciais para a definição da pena, acrescentamos, no **§ 1º**, a necessidade de se levar em conta a aplicação gradativa, **proporcional** à gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator e a vantagem por ele auferida ou pretendida, a condição econômica do infrator, a reincidência, o grau do dano causado, a cooperação do infrator, e a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano. Esse conjunto permite melhor gradação das penas, trazendo circunstâncias atenuantes e agravantes que permitem a aplicação mais justa e equilibrada das sanções previstas.

Para **entidades e órgãos públicos**, entendemos ser apropriada a aplicação das sanções de advertência, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão parcial ou total de funcionamento de banco de dados, suspensão do exercício de atividade de tratamento e a proibição parcial ou total do exercício dessas atividades.

[Art. 53] – Criação do órgão competente

É consenso que uma aplicação da Lei Geral de Proteção de Dados Pessoais depende da criação de um órgão técnico, centralizado e com independência e autonomia administrativa e financeira para expedir normas complementares e fiscalizar o setor. Durante a tramitação deste Projeto ficou claro que, muito embora a cultura de proteção de dados pessoais vem aumentando na sociedade moderna, trata-se de um setor de grande complexidade técnica e elevada assimetria de informação entre titulares e agentes de tratamento. Nesse sentido, a proposta do Poder Executivo já previa a designação de um órgão competente para fiscalizar o setor, o que autoriza a apresentação de emendas parlamentares nesta área.

Acreditamos que algumas características do órgão são essenciais de serem determinadas nesta Lei Geral. A primeira delas é a mencionada independência. Com isso em mente, propomos nomear o órgão competente como **Autoridade Nacional de Proteção de Dados**, no âmbito da administração indireta. Como autarquia, referenciamos neste instrumento a forma de escolha dos seus dirigentes, bem como a gestão de seus recursos

humanos, aos ditames estabelecidos pela Lei das Agências, Lei nº 9.986, de 18 de julho de 2000.

Preocupados com uma política de eficiência e de razoabilidade da máquina pública, optamos por dotar a Autoridade de apenas três Conselheiros, com mandatos de 4 anos. Para que não coincidam os términos dos mandatos, estabelecemos mandatos distintos para os primeiros conselheiros indicados.

Por último, não obstante a criação do órgão ter sido abordada sob a ótica de se manter esta Lei Geral a mais concisa possível, incluímos a previsão de que ex-conselheiros não poderão utilizar de informações privilegiadas obtidas em decorrência do cargo exercido.

[Art. 54] – Atribuições do órgão competente

Para uma proteção de dados efetiva é necessário que o ente controlador possua as ferramentas regulatórias adequadas. Tendo em vista que o órgão responsável poderá aplicar penalidades, é necessário também estabelecer claramente o alcance de suas competências, assim como dotá-lo de receitas que garantam o seu funcionamento fiscalizatório. Dessa forma, evitam-se arbitrariedades ao mesmo tempo em que se garante a aplicação dos princípios, fundamentos e garantias previstos em Lei. Com este raciocínio as treze competências previstas em um dos projetos foram reajustadas, retirando-se excessos previstos originalmente e reforçando necessidades. Como resultado, as prerrogativas foram rearranjadas em dezesseis incisos.

Entre as modificações nas atribuições cabe destacar: o zelo pela observância do segredo comercial e industrial (**inciso II**); o atendimento a petições de titulares (**V**); solicitação de relatórios de impacto à proteção de dados para casos de alto risco (**XIII**); audiência dos agentes de tratamento e sociedade (**XIV**), arrecadação e aplicação de receitas (**XV**), e; realização de auditorias no âmbito da atividade de fiscalização (**XVI**).

Também nessa questão da fiscalização e da imposição de condicionamentos, optamos por deixar expresso, por meio de **parágrafo único**, que além dos princípios e garantias previstos nesta Lei, o artigo 170 da Constituição Federal, que fundamenta a **liberdade econômica e a livre iniciativa**, deverá nortear a atuação do órgão competente.

[Art. 55] – Receitas do órgão competente

Como dito anteriormente, um órgão somente poderá fiscalizar efetivamente um determinado setor da economia com verbas suficientes e perenes. Por outro lado, o ente regulador não pode se tornar simplesmente um novo elemento arrecadador. Por esses motivos, ao mesmo tempo em que prescrevemos claramente a separação de receitas orçamentárias próprias para o futuro órgão designado, determinamos oito fontes adicionais de recursos. Em tempo, esclarecemos que os oito incisos previstos nada mais são do que aqueles normalmente destinados a órgãos da administração direta ou indireta, tais como receitas com **dívida ativa**, **doações**, **mercado financeiro**, cobrança de **emolumentos,** acordos, **convênios ou contratos** e venda de **publicações**.

É importante observar que não se quer criar uma indústria da multa. Apenas se garantir a independência administrativa da Autoridade, e, com isso, assegurar o poder fiscalizatório do órgão.

[Art. 56] – Composição do Conselho Consultivo

O Conselho Consultivo é órgão que se reveste da maior importância para o correto balizamento das atividades a serem executadas pelo órgão competente. Por isso, a composição do conselho deve contribuir para melhor canalizar a diversidade de opiniões e necessidades dos principais setores, ou atores, da sociedade, para serem utilizados pela instituição pública. Por isso, entendemos que a composição do Conselho, originalmente prevista pelo Executivo, em 15 membros, dos quais 10 privativos a membros da União (2/3 ou 67%) e apenas 5 (1/3 ou 33%), a serem divididos entre o terceiro setor e as empresas do mercado, é extremamente desbalanceada em prol da visão da União. Esse desequilíbrio poderá resultar, por exemplo, em ações normativas e de elaboração de políticas públicas com focos, objetivos e utilização de recursos desajustados.

Por esses motivos buscamos realinhar os pesos dos setores. A inspiração para nossa proposta advém do Comitê Gestor da Internet, modelo, que apesar de em processo de reformas, possui sucesso histórico, aclamado internacionalmente. Naquele órgão, a **União** possui **40%** dos

assentos, a **sociedade civil** organizada **20%**, as **empresas** do setor **20%** e a **academia** os restantes **20%**. Assim, nossa readequação prevê 23 assentos que refletirá essa mesma proporcionalidade. Seis posições para o Poder Executivo e um para cada uma das demais instituições Federais – Senado Federal, Câmara dos Deputados, Conselho Nacional de Justiça e Conselho Nacional do Ministério Público. Mantivemos uma posição para o CGI e ampliamos para 4 cadeiras a representação da sociedade civil, a mesma quantidade reservada para a academia e o setor empresarial.

[Art. 58] – Entrada em vigência da Lei

As alterações propostas por esta Lei Geral no *modus operandi* dos diversos setores da economia que lidam com o processamento de dados pessoais são bastante significativas. O sistema bancário, de crédito, comércio, cadastros vários, assim como operadoras de serviços públicos ou privados, todos deverão se readequar e atender as exigências da nova Lei. Ademais, esta será a primeira legislação do país a tratar do tema de forma tão estruturada e pormenorizada. São indicadas obrigações, procedimentos e responsabilidades de acordo com as especificidades de cada agente que compõe a cadeia de tratamento de dados, quer sejam responsáveis, operadores ou encarregados, nos termos desta Lei.

Por esses motivos, em todas as Audiências Públicas os participantes foram unânimes em solicitar a ampliação do prazo. O maior prazo externado foi de 3 anos. No caso da recente Regulação europeia, o prazo para entrada em vigência foi de 2 anos. Concordamos com essa necessidade e entendemos que o **vacatio legis** deva ser ampliado, do originalmente encaminhado de 6 meses, para **1 ano e meio (dezoito meses)**.

[Art. 59] – Notificação de empresa estrangeira

Tendo em vista a natureza global do tratamento dos dados efetuados pelas empresas de TIC, compreendemos a problemática relatada reiteradamente nesta Comissão da dificuldade de se notificar empresas estrangeiras. Assim, incluímos o **art. 59** determinando que essas empresas serão notificadas através de seu escritório no país, independente da forma em que operem no Brasil, quer seja por meio de filial, escritório de

representação ou outras.

[Art. 60] – Dados da educação

A Lei de Diretrizes e Bases da Educação (LDB - Lei nº 9.394/96) estabelece que a União deverá ter acesso a todos os dados e informações de todos os estabelecimento e órgãos educacionais. Para o sistema de ensino superior, a Lei do Sistema Nacional de Avaliação da Educação Superior – SINAES (Lei nº 10.861/04), estabeleceu ordenamento similar. Na coordenação dessa base informacional encontra-se o INEP (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira). Assim, como no caso da saúde, discutido anteriormente, os dados relativos à educação dos alunos nas diversas etapas de formação, que incluem desempenho escolar em cada matéria, assim como nome, filiação e endereço, possuem um valor importantíssimo. Da mesma forma que a posse destes danos possuem alto potencial de gerar dano a direitos fundamentais das pessoas, este conjunto também é extremamente importante para a geração e formulação, não só de políticas públicas, mas, também de pesquisas das mais diversas. Assim, também considerando a complexidade deste sub-conjunto de dados pessoais e dos atores envolvidos, entendemos que tanto o **órgão competente, quanto o INEP deverão emitir regulamentação**, no âmbito de suas competências.

[Art. 61] – Adequação do Marco Civil da Internet

O objetivo do Marco Civil da Internet foi transpor para o mundo da internet as garantias e os direitos individuais garantidos na Constituição e assim, manter as principais características da rede mundial, entre outras a pluralidade, abertura, colaboração e neutralidade. Apenas com o intuito de **recepcionar no Marco a previsão explicita à esta Lei** de proteção de dados, determinamos alterar o inciso X do art. 7º e inciso II, do art. 16 daquele diploma legal.

[Art. 62] – Adequação desta Lei ao ordenamento jurídico pátrio

Por último, incluímos como artigo final um dispositivo em que indica, de

maneira clara e inequívoca, que os ditames desta Lei Geral, vêm para serem adicionados ao **arcabouço legal já existente**. Ao longo deste texto, tivemos a precaução de não alterar os ditames do consagrado Código de Defesa do Consumidor, do Código Civil, da Lei de Acesso à Informação, ou ainda do Marco Civil da Internet. Entretanto, julgamos pertinente esclarecer o princípio aditivo deste diploma ao ordenamento jurídico do País.

9. Análise das Emendas Oferecidas ao PL 5.276/16

EMP nº 1, Dep. Weverton Rocha: somos pela **REJEIÇÃO**, porque obrigar a formulação de regras de boas práticas não condiz com os princípios fundamentais da autorregulação. Ademais, gera aumento do fardo regulatório, do custo dos processos internos das empresas (*compliance*) e potencial criação de reserva de mercado para empresas especialistas nessa atividade.

EMP nº 2, Dep. Weverton Rocha: somos pela **REJEIÇÃO**, porque, uma vez que não há disposição em contrário, juízes já detêm competência para determinar eventualmente, e nos termos da presente proposição, o término de tratamento de dados. Até porque o art. 5º, XXXV, da Constituição Federal dispõe que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".

EMP nº 3, Dep. Weverton Rocha: somos pela **APROVAÇÃO**, porque concordamos com os argumentos de que a Lei deve estabelecer de forma exaustiva as exceções para a conservação de dados eliminados e não conceder sem restrições tal poder, excessivo, ao órgão competente.

EMP nº 4, Dep. Jorge Tadeu Mudalen: somos pela **REJEIÇÃO**, porque a supressão do termo "informado" como requer o autor enfraquece o exercício do direito do titular de ter conhecimento detalhado acerca das consequências, positivas e negativas, de se optar por consentir com o tratamento de seus dados. É imperioso resguardar a simetria de informações entre o titular e o responsável pela atividade de tratamento de dados pessoais.

EMP nº 5, Dep. Leonardo Quintão: somos pela **APROVAÇÃO PARCIAL**. Concordamos com o autor de que o objetivo do § 1º

do art. 7º seja a comunicação ao titular, portanto estamos de acordo com a redação sugerida. Por outro lado, não concordamos que o órgão competente não possa regulamentar a questão de como os titulares possam ser informados. Entendemos que há outros dispositivos que limitam ingerência excessiva da Administração nas atividades do setor.

EMP nº 6, Dep. Sandro Alex: somos pela **APROVAÇÃO PARCIAL**, porque discordamos com o entendimento de que permitir ao órgão regulador realizar auditoria em entidades envolvidas com o tratamento de dados pessoais é excessivo e exorbita a esfera de competência de órgão regulador. A auditoria é prevista, por exemplo no regramento europeu e é instrumento apropriado para uma efetiva fiscalização do órgão competente. Da mesma forma, no Brasil, o Banco Central, por exemplo, de acordo com seu Manual da Supervisão, quando realiza processos de supervisão, inspeciona as instituições por meio de reuniões, visitas a setores, análise de bases de dados, de documentos, de procedimentos e processos, e de sistemas e estruturas, assim como requer a elaboração de papéis de trabalho. Temos a compreensão de que o mesmo nível de fiscalização é necessário, pois seria a única forma de se verificar os métodos e processos utilizados para mitigação de riscos em bases de dados e sistemas informatizados.

Sob outro aspecto das competências, entendemos também que as formas em que a publicidade das operações deverá se dar é da esfera do regulador, mas inserimos a necessidade de que se preserve a proteção aos segredos comercial e industrial. Concordamos, por fim, que o termo “normas complementares” é excessivamente genérico, podendo levar a arbitrariedades e criar insegurança jurídica. Com esse intuito inserimos a competência de “editar **regulamentos** e procedimentos sobre proteção de dados pessoais e privacidade”, o que circunscreve mais precisamente a extensão da regulação infralegal.

EMP nº 7, Dep. Paes Landim: somos pela **APROVAÇÃO**, com adequação nos termos, porque concordamos com o argumento de que o compartilhamento de dados com entidades privadas deva se dar apenas quando previsto em Lei e respaldados em convênios específicos.

EMP nº 8, Dep. Paes Landim: somos pela **REJEIÇÃO**, por entendermos que a expressão “proteção ao crédito” é por demais ampla, podendo ensejar interpretações extensivas e fragilizando o direito ao sigilo

financeiro dos titulares cuja proteção à privacidade é o objetivo principal dessa Lei.

EMP nº 9, Dep. Paes Landim: somos pela **APROVAÇÃO**, pois entendemos que todos os casos de informação ao titular e ao órgão competente devam respeitar e observar os eventuais segredos comercial e industrial.

EMP nº 10, Dep. Paes Landim: somos pela **REJEIÇÃO**, por termos a convicção de que dados biométricos, quando vinculados a pessoa natural, são sensíveis em qualquer aplicação. Portanto, sua importância não pode ser relativizada, como pretende o autor da proposta.

EMP nº 11, Dep. Paes Landim: somos, no mérito, pela **APROVAÇÃO**. Entretanto, sua recepção se dá pela nova definição de dados anonimizados e de anonimização adotadas no Substitutivo, que inclui os termos “considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Dessa forma, a redação dada ao § 1º, do art. 13, que determina que dados de perfil comportamental poderão ser considerados como pessoais se identificada a pessoa natural, atende, no mérito, a Emenda sugerida.

Essas são as alterações que propomos na forma de SUBSTITUTIVO.

10. Conclusão e Voto

Por fim e pelos motivos apresentados, somos pela APROVAÇÃO aos Projetos de Lei nºs 4.060/12, 5.276/16 e 6.291/16 e pela APROVAÇÃO das Emendas nºs 3, 7, 9 e 11 e pela APROVAÇÃO PARCIAL das Emendas nºs 5 e 6, todas elas apresentadas ao PL nº 5.276/16, na forma de SUSBSTITUTIVO, e pela REJEIÇÃO das Emendas nºs 1, 2, 4, 8 e 10, estas também apresentadas ao PL nº 5.276/16.

Sala da Comissão, em de de 2018.

Deputado Orlando Silva
Relator

COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI Nº 4060, DE 2012

(TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS)

SUBSTITUTIVO AO PROJETO DE LEI Nº 4.060, DE 2012

(Apenso PLs nºs 5.276/16 e 6.291/16)

Estabelece a Lei Geral de Proteção de Dados.

O Congresso Nacional decreta:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

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

Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:

I – a autodeterminação informativa;

II – a liberdade de expressão, de informação, de comunicação e de opinião;

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

IV – o desenvolvimento econômico, tecnológico e a inovação;

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

VI – os direitos humanos e o livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

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

I – a operação de tratamento seja realizada no território nacional, salvo o tratamento previsto no inciso IV do art. 4º;

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

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

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

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I – realizado por pessoa natural para fins exclusivamente pessoais;

II – realizado para fins exclusivamente:

a) jornalísticos e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11;

III – realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais; ou

IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observado o devido processo legal e observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente e que deverão observar a limitação imposta no § 4º.

§ 3º Órgão competente emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III poderão ser tratados por pessoa de direito privado.

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

I – dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

II – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural;

III – dados anonimizados: dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

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

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

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

VIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação entre o responsável e os titulares e o órgão competente;

IX – agentes do tratamento: o responsável e o operador;

X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI – anonimização: utilização de meios técnicos razoáveis e disponíveis quando do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

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

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro ou organização internacional da qual o país seja membro;

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

XVII – relatório de impacto à proteção de dados pessoais: documentação do responsável que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou

estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XIX – órgão competente: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

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

I – finalidade: pelo qual o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;

II – adequação: pelo qual o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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

IV – livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais;

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

VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do

tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX – não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: pelo qual o agente deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, incluindo a eficácia das medidas.

CAPÍTULO II

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I

Requisitos para o tratamento

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo responsável;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres e nos termos do Capítulo IV;

IV – para a realização de estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, nos termos da Lei nº 9.307, de 23 de setembro de 1996;

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII – para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para proteção do crédito de acordo com o art. 43 da Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor.

§ 1º Nos casos de aplicação do disposto nos incisos II e III e excetuadas as hipóteses previstas no art. 4º, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do art. 23 poderá ser especificada pelo órgão competente.

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.

§ 4º Fica dispensada a exigência do consentimento previsto no caput para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e princípios previstos nesta Lei.

§ 5º O responsável que obteve o consentimento a que faz referência o inciso I que necessitar comunicar ou compartilhar dados pessoais com outros responsáveis deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º 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. 8º O consentimento previsto no art. 7º, inciso I, deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, este deverá ser provido em cláusula destacada de demais cláusulas contratuais.

§ 2º Cabe ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vicio de consentimento.

§ 4º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§ 5º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do art. 18.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º, o responsável deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I – finalidade específica do tratamento;

II – forma e duração do tratamento, observados os segredos comercial e industrial;

III – identificação do responsável;

IV – informações de contato do responsável;

V – informações acerca do uso compartilhado de dados pelo responsável e a finalidade;

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita aos direitos contidos no art. 18.

§ 1º Na hipótese em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenham

conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, havendo mudanças da finalidade para o tratamento de dados pessoais não compatível com o consentimento original, o responsável deverá informar previamente ao titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações..

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem:

I – o apoio e a promoção de atividades do responsável; e

II – em relação ao titular, a proteção do exercício regular de seus direitos ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse.

§ 3º O órgão competente poderá solicitar ao responsável relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento o seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Dados Sensíveis

Art. 11. É vedado o tratamento de dados pessoais sensíveis, exceto:

I – com fornecimento de consentimento específico e em destaque, pelo titular, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de uma obrigação legal pelo responsável;

b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos inclusive em contrato, processo judicial, administrativo ou arbitral, nos termos da Lei nº 9.307, de 23 de setembro de 1996;

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; ou

g) garantir a prevenção à fraude e a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º e exceto no caso no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do art. 23.

§ 3º A comunicação ou o uso compartilhado de dados sensíveis entre responsáveis, com o objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte do órgão competente, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas respectivas competências.

Art. 12. Os dados anonimizados serão considerados dados pessoais, para os fins desta Lei, quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessário para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para a formação do perfil comportamental de uma determinada pessoa natural, se identificada.

§ 3º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização, e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de

realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudomização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou pesquisa de que trata o caput em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput, não sendo permitida, em qualquer circunstância, a transferência dos dados a terceiros.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte do órgão competente e das autoridades da área de saúde e sanitárias, no âmbito de suas respectivas competências.

§ 4º Para os efeitos deste artigo a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão através do uso de informação adicional mantida separadamente pelo responsável em ambiente controlado e seguro.

Seção III

Crianças e Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal.

§ 2º Os responsáveis pelo tratamento de dados de que trata o § 1º deverão manter pública informação sobre os tipos de dados coletados, como estes são utilizados e os procedimentos para o exercício dos direitos a que se refere o art. 18.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º quando a coleta se faça necessária para contatar os pais ou responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção e em nenhum caso poderão ser repassados a terceiros sem o consentimento de que trata o § 1º.

§ 4º Os responsáveis por tratamento de dados não devem condicionar a participação dos titulares de que trata o § 1º a jogos, aplicações de internet ou outras atividades ao fornecimento de mais informações pessoais que as estritamente necessárias para participar da atividade.

§ 5º O responsável deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º foi dado pelo responsável pela criança, levando em consideração as tecnologias disponíveis.

§ 6º As informações referentes ao tratamento de dados referidas no § 3º deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptiva, sensoriais, intelectuais e mentais do usuário, utilizando recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou responsável legal e também adequadas ao entendimento da criança.

Seção IV

Término do tratamento

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º, resguardado o interesse público; ou

IV – determinação do órgão competente, quando houver violação da legislação em vigor a respeito.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal do responsável;

II – estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização dos dados pessoais;

III – transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV – para uso exclusivo do responsável, sendo vedado o seu acesso por terceiros e desde que anonimizados.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do responsável em relação aos dados por ele tratados, a qualquer momento e mediante requisição, em relação aos seus dados:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V – portabilidade de seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão responsável;

VI – eliminação, de dados pessoais com cujo tratamento o titular tenha consentido, exceto nas hipóteses previstas no art. 16;

VII – a informação das entidades públicas e privadas com as quais o responsável realizou uso compartilhado de dados;

VIII – a informação da possibilidade de não fornecer o consentimento e sobre as consequências da negativa;

IX – a revogação do consentimento nos termos do § 5º do art. 8º; e

X – peticionar contra responsável perante o órgão competente e os organismos de defesa do consumidor.

§ 1º O titular pode se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular, representantes legalmente constituídos, a um dos agentes de tratamento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º, o responsável enviará ao titular resposta em que poderá:

I – comunicar que não é agente de tratamento dos dados, indicando, sempre que possível, o agente; ou

II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 4º O requerimento de que trata o § 2º será atendido sem custos para o titular nos prazos e termos previstos na regulamentação.

§ 5º O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

§ 6º A portabilidade dos dados pessoais a que se refere o inciso V do caput não inclui dados que já tenham sido anonimizados pelo responsável.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até quinze dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para tal fim; ou

II – sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais, observado o segredo comercial e industrial, nos termos da regulamentação do órgão competente, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º O órgão competente poderá dispor de forma diferenciada acerca dos prazos dos incisos I e II do caput para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, 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 pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade.

§ 1º O responsável deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º baseado na observância de segredo comercial e industrial, o órgão competente poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizados de dados pessoais.

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos 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 art. 81 e art. 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.

CAPITULO IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

Tratamento de Dados Pessoais pelo Poder Público

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuição legal pelo serviço público, desde que:

I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, finalidade, procedimentos e práticas utilizadas para a execução dessas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II – sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, no âmbito da Lei que menciona o caput, sendo vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado; e

III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

§ 1º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput de instituir as autoridades de que trata a Lei que menciona o caput.

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o poder público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997, da Lei nº 9.784, de 29 de janeiro de 1999 e da Lei nº 12.527, de 18 de novembro de 2011.

Art. 24. As empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução desta, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado para a execução de políticas públicas, prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I – em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011;

II – quando houver previsão legal e a transferência seja respaldada em contratos, convênios ou instrumentos congêneres.

III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

§ 2º Os contratos e convênios de que trata o § 1º deverão ser comunicados ao órgão competente.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:

I – nas hipóteses de dispensa do consentimento previstas nesta Lei;

II – nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do art. 23 desta Lei; ou

III – nas exceções constantes no § 1º do art. 26.

Art. 28. A comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do art. 23 desta Lei.

Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação ou o uso compartilhado de dados pessoais.

Seção II

Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto à proteção de dados pessoais e poderá sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

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

II – quando o responsável oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta lei, na forma de:

a) cláusulas contratuais específicas para uma determinada transferência;

b) cláusulas contratuais padrão;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III – quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V – quando o órgão competente autorizar a transferência;

VI – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do art. 23 desta Lei;

VIII – quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX – quando necessário para atender as hipóteses previstas no art. 7º, inciso II, V e VI.

Parágrafo único. Para os fins do inciso I do art. 33 desta Lei, pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer ao órgão competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou da organização internacional mencionado no inciso I do art. 33, será avaliado pelo órgão competente, que levará em conta:

I – as normas gerais e setoriais da legislação em vigor no país de destino ou na organização internacional;

II – a natureza dos dados;

III – a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV – a adoção de medidas de segurança previstas em regulamento;

V – as outras circunstâncias específicas relativas à transferência; e

VI – a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.

Art. 35. A definição do conteúdo de cláusulas contratuais padrão, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do art. 33, será realizado pelo órgão competente.

§ 1º Para a verificação do previsto no caput deste artigo deverão ser considerados os requisitos, condições e garantias mínimas para a transferência que observe os direitos, garantias e princípios desta lei;

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º O órgão competente poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pelo órgão competente e, caso em desconformidade com esta Lei, submetidos à revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos § 1º e § 2º do art. 46.

Art. 36. Alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 deverão ser comunicadas ao órgão competente.

CAPÍTULO VI

DOS AGENTES DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Responsável e operador

Art. 37. O responsável e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse

Art. 38. O órgão competente poderá determinar ao responsável que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, nos termos do regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para sua coleta e para a garantia da segurança das informações, bem como a análise do responsável com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

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.

Art. 40. O órgão competente poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso dos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Encarregado pelo tratamento de dados pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do responsável.

§ 2º As atividades do encarregado consistem em:

I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações do órgão competente e adotar providências;

III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – demais atribuições determinadas pelo responsável ou estabelecidas em normas complementares.

§ 3º O órgão competente poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Seção III

Responsabilidade e ressarcimento de danos

Art. 42. O responsável ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º. A fim de assegurar a efetiva indenização ao titular dos dados:

I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável, hipótese em que o operador equipara-se a responsável, salvo as hipóteses de exclusão do art. 43.

II – responsáveis que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo as hipóteses de exclusão do art. 43.

§ 2º 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,

houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos, que tenham por objeto a responsabilização nos termos do caput, podem ser exercidas a título coletivo em juízo, nos termos do Título III, da Lei 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;

III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I – o modo pelo qual é realizado;

II – o resultado e os riscos que razoavelmente dele se esperam;

III – as técnicas de tratamento de dados pessoais disponíveis à época em que realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o responsável ou o operador, que ao deixar de adotar as medidas de segurança previstas no art. 43, der causa ao dano.

Art. 45. As hipóteses de violação ao direito do titular no âmbito das relações de consumo permanecem inteiramente sujeitas às regras de responsabilidade previstas na Lei 8.078, de 11 de setembro de 1990, observado o inciso III do art. 4º daquela lei.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Segurança e sigilo de dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º O órgão competente poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis, assim como os princípios previstos no art. 6º desta Lei.

§ 2º As medidas de que trata o caput deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a assegurar a

segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O responsável deverá comunicar ao órgão competente e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e deverá mencionar, no mínimo:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV – os riscos relacionados ao incidente;

V – os motivos da demora, no caso da comunicação não ter sido imediata; e

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

§ 2º O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de providências, como:

I – ampla divulgação do fato em meios de comunicação; e

II – medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, padrões de boas práticas e de governança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Boas práticas e Governança

Art. 50. Os responsáveis e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios, decorrentes de tratamento de dados de titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII, do art. 6º, desta Lei, o responsável poderá, observada a estrutura, escala e volume de suas operações, bem como a sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos para os titulares dos dados:

I – implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do responsável em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo em que se deu sua coleta;

c) seja adaptado à estrutura, escala e volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas a partir de processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado, e em especial, a pedido do órgão competente ou de outra entidade responsável por promover o cumprimento boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pelo órgão competente.

Art. 51. O órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

CAPÍTULO VIII

DA FISCALIZAÇÃO

Seção I

Sanções administrativas

Art. 52. As infrações realizadas por agentes de tratamento de dados às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa simples ou diária, de até 4% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais), por infração;

III – publicização da infração após devidamente apurada e confirmada a sua ocorrência;

IV – bloqueio de dados pessoais a que se refere a infração, até a sua regularização;

V – eliminação de dados pessoais a que se refere a infração; e

VI – suspensão parcial ou total de funcionamento de banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogáveis por igual período até a regularização da atividade de tratamento pelo responsável;

VII – suspensão do exercício de atividade de tratamento de dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogáveis por igual período;

VIII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;

§ 1º As sanções serão aplicadas, após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e:

I – a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II – a boa fé do infrator;

III – a vantagem auferida ou pretendida pelo infrator;

IV – a condição econômica do infrator;

V – a reincidência;

VI – ao grau do dano;

VII – a cooperação do infrator;

VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 3º O disposto nos incisos I e de III a VIII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do

disposto nas Leis nºs 8.112, de 11 de dezembro de 1990, 8.429, de 2 de junho de 1992 e 12.527, de 18 de novembro de 2011.

Seção II

Órgão competente e Conselho Nacional de Proteção de Dados e da Privacidade

Art. 53. Fica criado o órgão competente, Autoridade Nacional de Proteção de Dados, entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça.

§ 1º A Autoridade deverá ser regida nos termos previstos na Lei nº 9.986, de 18 de julho de 2000.

§ 2º A Autoridade terá como órgão máximo o Conselho Diretor, o Conselho Nacional de Proteção de Dados e da Privacidade, além das unidades especializadas para a aplicação desta Lei.

§ 3º A natureza de autarquia especial conferida à Autoridade é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira.

§ 4º O regulamento e a estrutura organizacional da Autoridade serão aprovados por decreto do Presidente da República.

§ 5º O Conselho Diretor será composto por três conselheiros e decidirá por maioria.

§ 6º O mandato dos membros do Conselho Diretor será de quatro anos.

§ 7º Os mandatos dos primeiros membros do Conselho Diretor serão de três, quatro, cinco anos, a serem estabelecidos no decreto de nomeação.

§ 8º É vedado ao ex-conselheiro utilizar informações privilegiadas obtidas em decorrência do cargo exercido, sob pena de incorrer em improbidade administrativa.

Art. 54. O órgão competente terá as seguintes atribuições:

I – zelar pela proteção dos dados pessoais, nos termos da legislação;

II – zelar pela observância do segredo comercial e industrial em ponderação com a proteção de dados pessoais, e do sigilo das informações quando protegido por lei ou quando violar os fundamentos do art. 2º desta Lei;

III – elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;

IV – fiscalizar e aplicar sanções em caso de tratamento de dados em descumprimento com a legislação, mediante processo administrativo que assegure o contraditório e a ampla defesa;

V – atender petições de titular contra responsável;

VI – promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

VII – promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, que deverão levar em consideração especificidades das atividades e o porte dos responsáveis;

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

X – dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento, observando o respeito ao segredo comercial e industrial;

XI – solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII – elaborar relatórios anuais acerca de suas atividades;

XIII – editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; e

XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante, assim como prestar contas sobre suas atividades e planejamento;

XV – arrecadar e aplicar suas receitas;

XVI – realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais realizado pelos agentes de tratamento, incluindo o Poder Público.

Parágrafo único. Ao impor condicionamentos administrativos ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, o órgão competente deve observar a exigência

de mínima intervenção, assegurando fundamentos, princípios e direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

Art. 55. Constituem receitas do órgão competente:

I – o produto da execução da sua dívida ativa;

II – as dotações consignadas no Orçamento-Geral da União, créditos especiais, créditos adicionais, transferências e repasses que lhe forem conferidos;

III – as doações, legados, subvenções e outros recursos que lhe forem destinados;

IV – os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade;

V – os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo;

VI – produto da cobrança de emolumentos por serviços prestados;

VII – recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais e internacionais;

VIII – produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

Art. 56. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:

I – seis representantes do Poder Executivo Federal;

II – um representante indicado pelo Senado Federal;

III – um representante indicado pela Câmara dos Deputados;

IV – um representante indicado pelo Conselho Nacional de Justiça;

V – um representante indicado pelo Conselho Nacional do Ministério Público;

VI – um representante indicado pelo Comitê Gestor da Internet no Brasil;

VII – quatro representantes da sociedade civil com atuação comprovada em proteção de dados pessoais;

VIII – quatro representantes de instituição científica, tecnológica e de inovação ; e

IX – quatro representantes de entidade representativa do setor empresarial afeito à área de tratamento de dados pessoais.

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação, e terão mandato de dois anos, permitida uma recondução.

§ 2º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público, não remunerada.

§ 3º Os representantes referidos no inciso I a VI do caput e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 4º Os representantes referidos nos incisos VII a IX do caput e seus respectivos suplentes serão indicados na forma do regulamento e não poderão ser membros da entidade mencionada no inciso VI.

Art. 57. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e de atuação do órgão competente;

II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III – sugerir ações a serem realizadas pelo órgão competente;

IV – realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e

V – disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.

CAPÍTULO IX

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 58. Esta Lei entra em vigor 18 (dezoito) meses após a data de sua publicação.

Parágrafo único. O órgão competente estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento e a natureza dos dados.

Art. 59. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 60. O órgão competente e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), no âmbito de suas

respectivas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º, do art. 9º, da Lei no 9.394, de 20 dezembro de 1996, que estabelece as diretrizes e base da educação nacional, e os referentes ao Sistema Nacional de Avaliação da Educação Superior – SINAES, de que trata a Lei nº 10.861, de 14 de abril de 2004.

Art. 61. O inciso X, do art. 7º, e o inciso II, do art. 16, da Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, passarão a vigorar com a seguinte redação:

"Art.7º .....

.....

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 e na que trata da proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que trata da proteção de dados pessoais." (NR)

Art. 62. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria

ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Sala da Comissão, em de de 2018.

Deputado Orlando Silva
Relator