Double Blind Review pelo SEER/OJS
Recebido em: 10.08.2019
Aprovado em: 18.08.2019

Revista de Direito, Governança e Novas Tecnologias

A SALVAGUARDA DA PRIVACIDADE E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

THE PRIVACY SAFEGUARD AND THE NATIONAL DATA PROTECTION AUTHORITY

Rafael Copetti*

José Renato Gaziero Cella**

RESUMO

O artigo analisa a proteção de dados pessoais no Brasil e tem como objetivo analisar, por meio do método hipotético-dedutivo, as características normativas da legislação que atualmente prevê a criação de uma Autoridade Nacional de Proteção de Dados, especialmente a partir da edição da Medida Provisória nº 869/2018. É analisado se referido instrumento jurídico trouxe meios adequados para salvaguardar o direito fundamental à privacidade e proteção dos dados pessoais. Ao final, percebe-se que o texto retira características indispensáveis à atuação do ente criado, comprometendo a segurança desses direitos.

Palavras-chave: Proteção de dados pessoais; Autoridade Proteção; Medida Provisória; Independência; Subordinação.

ABSTRACT

The article analyzes the personal data protection in Brazil and aims to analyse, through the hypothetical-deductive method, the normative characteristics of the legislation that currently provides for the creation of a National Data Protection Authority, especially from the edition of the Measure Provisional nº 869/2018. It is analyzed if the legal instrument has provided adequate means to safeguard the fundamental right to privacy and protection of personal data. At the end, it is perceived that the text removes essential characteristics to the performance of the created entity, compromising the security of that rights.

Keywords: Personal Data Protection; Protection Autority; Provisional Measure; Independency; Subordination.

1. INTRODUÇÃO

Na era da informação o tema proteção dos dados pessoais ganha ainda mais relevância, pois a facilidade do acesso a dados e informações e a utilização de recursos e mídias sociais os deixam vulneráveis.

É preciso que os instrumentos normativos estejam em consonância com a aludida

* Mestre em Direito, Democracia e Sustentabilidade pela IMED de Passo Fundo/RS. Especialista em Direito Público pela Faculdade Meridional - IMED/ESMAFE. Professor de Direito na FABE Marau. Servidor Público Federal TRE-RS.

** Doutor em Filosofia e Teoria do Direito pela UFSC. Mestre em Direito pela UFPR. Professor do Programa de Pós-Graduação *Stricto Sensu* em Direito da Faculdade Meridional - PPGD/IMED, Passo Fundo-RS.

mutabilidade social oriunda célere evolução tecnológica. É importante que as normativas acompanhem as novas descobertas científicas, devendo, quando menos, existirem diretrizes transparentes e objetivas que permitam a adaptação legislativa.

No Brasil, no ano de 2018, ainda que com atraso, foi publicada a Lei Geral de Proteção de Dados Pessoais. Contudo, consoante entendimento da Presidência da República, apresentava vício de iniciativa em determinados dispositivos, sendo vetado, por exemplo, os dispositivos que instituíam a Autoridade de Proteção de Dados Pessoais.

Nesse contexto que, posteriormente, ao final do mandato do último governo foi criada a Autoridade Nacional de Proteção de Dados (ANPD), por meio de uma Medida Provisória, dando-se uma nova roupagem à autoridade inicialmente prevista na lei de dados do Brasil. O uso desse instrumento jurídico de certa forma retira do âmbito do Poder Legislativo a possibilidade de discussão da matéria, local devidamente adequado para tal finalidade.

Assim, o problema de pesquisa resulta da necessidade de se analisar se a Medida Provisória nº 869/2018 trouxe instrumentos jurídicos adequados para salvaguardar o direito fundamental à privacidade e proteção dos dados pessoais.

Como hipótese a ser analisada está que a Medida Provisória nº 869 compromete a atuação efetiva e eficaz da Autoridade de Proteção de Dados brasileira.

O artigo, portanto, visa analisar as características normativas da legislação que atualmente prevê a criação de uma Autoridade Nacional de Proteção de Dados, perpassando pela análise de elementos considerados essenciais a esse ente e à proteção do direito à privacidade.

Com efeito, modelos de governos tecnocratas, visando alcançar seus ideais de eficiência, enxergam no compartilhamento de bancos de dados um bem em si mesmo. E esse modo de pensar e agir mostra-se um perigoso caminho rumo ao intercâmbio de dados pessoais sem que se considerem contrapesos e salvaguardas.

2. A DESEJAVEL PROTEÇÃO DE DADOS

A especificação da finalidade e a limitação do uso são princípios básicos de leis internacionais dessa matéria e também dede o Projeto de Lei para a Proteção de Dados

Pessoais que tramitou perante o Congresso Nacional. A noção subjacente é a de que o uso de informações pessoais deve servir à finalidade comunicada na coleta e a outros propósitos compatíveis, nos limites do consentimento do indivíduo.

Com efeito, a finalidade integra os princípios enumerados por Rodotà (2008, p. 60) como norteadores da proteção de dados pessoais, quais sejam:

> *princípio da correção* na coleta de dados e no tratamento das informações;
> *princípio da exatidão* dos dados coletados, acompanhado pela obrigação de sua utilização;
> *princípio da finalidade* da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a utilização dos dados (*princípio da utilização não-abusiva*); na eliminação ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);
> *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> *princípio da segurança* física e lógica da coleta dos dados.

É por isso que um programa de compartilhamento de dados não pode só ser justificado em termos de eficiência de gestão do Estado, como o governo até agora o fez. Ele precisa instituir garantias aos indivíduos afetados, sob pena de já nascer em descompasso com as discussões mais recentes sobre proteção de dados pessoais, que inclusive vê ocorrendo no Congresso Nacional.

Ressalte-se que, independentemente da definição de privacidade que se adote, deve-se ter uma ampliação da tutela da esfera privada dos sujeitos em virtude do tipo e quantidade de informações que são coletas e, como consequência, gerado um dano ao indivíduo.

Para melhor exemplificação, Rodotà (2008, p. 129) traz efeitos do panorama tecnológico essenciais à privacidade, e a define de forma singela como "*o direito de manter o controle sobre as próprias informações"* (RODOTÀ, 2008, p. 92):

> a) impõe como direito fundamental;
> b) especifica-se como direito à autodeterminação informativa e, mais precisamente, como direito a determinar as modalidades de construção da esfera privada na sua totalidade;

> c) apresenta-se, por fim, como precondição da cidadania na era eletrônica e, como tal, não pode ser confiada unicamente à lógica da auto-regulamentação ou das relações contratuais.

A justificativa trazida pelo autor para estipular tais características inerentes à privacidade é a de que "a descrição de um novo panorama tecnológico e as transformações que traz consigo, se apresentam como um caminho que deve ser percorrido para à plena compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação" (RODOTÀ, 2008, p. 127).

Ou seja, "como vivemos em um mundo onde as informações estão divididas com uma pluralidade de sujeitos e a coleta de informações que anteriormente era realizada através de cessões vindas de relações interpessoais e agora ocorre através de transações abstratas, passa-se de um mundo no qual o problema era o controle do fluxo das informações que saiam de dentro da esfera privada em direção ao exterior, para um mundo no qual o problema é o controle das informações que entram, tal como demonstra a autodeterminação do direito de não saber, pela atribuição dos indivíduos do poder de recusar interferências em sua esfera privada" (RODOTÀ, 2008, p. 128).

Todavia, assumindo os efeitos e seguindo os aspectos da privacidade trazidos por Rodotà, a definição do direito à privacidade compatível com a era moderna-tecnológica se dá como o direito fundamental à autodeterminação e ao controle informativo, decidindo, em sua totalidade, os dados informativos que constroem, adentram e saem da esfera privativa, apresentando-se como precondição da cidadania na era moderna, não sendo restrito à lógica da auto-regulamentação ou das relações contratuais, justificando-se à compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação e de um conjunto de condicionamentos.

Porém, como "vivemos em um mundo no qual aumenta o valor agregado das informações pessoais, onde a referência ao valor da pessoa em si e de sua dignidade passou a ser secundário em relação à transformação da informação em mercadoria" (RODOTÀ, 2008, p. 128), o desafio para aplicação do direito à privacidade é constante.

Informações de todos os tipos são coletadas mediante programas ou objetos de interação social. Seja pelo computador ou pelo *smartphone*, o acesso à uma rede social ou a algum sítio eletrônico da internet, na maioria das vezes se realiza uma pequena coleta de

dados por meio de *cookies*[†] de quem o está utilizando ou acessando para com algum objetivo proposto (expressamente) pelos desenvolvedores, e aceito (tácita ou expressamente) pelos usuários.

"O aumento da quantidade de informações pessoais coletadas por instituições públicas e privadas através de aplicativos de *smartphones* ou no acesso em rede, de forma geral, visa sobretudo à dois objetivos: por parte dos poderes púbicos, a aquisição de elementos necessários à gestão de programas de intervenção, e o desenvolvimento de estratégias empresariais privadas; conjuntamente ao controle da conformidade da população à gestão política dominante ou aos comportamentos prevalecentes" (RODOTÀ, 2008, p. 28).

Assim, a caracterização da organização social como uma sociedade com bases na acumulação e circulação das informações torna-se clara, trazendo novas situações e tipos de poder. Este, contudo, problemático ao ser legitimado e fundado na informação.

Tais desafios dão-se, "primeiramente, em virtude e a dificuldade de individualizar certos tipos de informações das quais o cidadão estaria disposto a renunciar definitivamente a controlar o seu tratamento e a atividade dos sujeitos que a utilizam, pois publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Em segundo lugar, a nova situação determinada pelo uso de computadores no tratamento das informações pessoais faz-se mais difícil caracterizar o cidadão como simples 'fornecedor de dados', sem que a ele caiba algum poder de tutela e tratamento dessas informações" (RODOTÀ, 2008, p. 36).

"As informações coletadas, além fazer as organizações públicas e privadas capazes de planejar e executar os seus programas, ainda permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes" (RODOTÀ, 2008, p. 37).

Daí a importância da proteção jurídica da privacidade, da vida privada ou da intimidade, cuja definição é trazida por Doneda (2006, p. 101):

> Ao se tratar da privacidade, há de se fazer antes de tudo um esclarecimento inicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representa-la , propriamente ou não, é considerável; além de

[†] "Um *cookie* é um pequeno texto que os sites podem enviar aos navegadores, anexado a qualquer conexão. Nas visitas posteriores o navegador reenvia os dados para o servidor dono do *cookie*. Um *cookie* é transmitido até que perca a validade, que é definida pelo site. Os sites geralmente usam os *cookies* para distinguir usuários e memorizar preferências." Cf: http://br.mozdev.org/firefox/cookies. Acesso em 28.out. 2016.

> 'privacidade' propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como 'privatividade' e 'privaticidade', por exemplo. O fato da doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas.

De acordo com Limberger (2007, p. 116), a intimidade como direito fundamental tem sua gênese na "[…] dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional". Para a autora, "[…] As exigências do mundo tecnológico atual fizeram com que o direito tutelasse essa nova face da intimidade. A intimidade deriva da dignidade humana, é um direito fundamental que integra a personalidade. Das relações da informática e a intimidade se desenvolve a autodeterminação informativa. […]" (LIMBERGER, 2007, p. 119).

Para Rodotá (1995, p. 122), a privacidade é "[…] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada […]".

No direito brasileiro, o direito à privacidade pode ser entendido como um direito da personalidade de matiz constitucional, com expressa previsão no artigo 5º, inciso X, da Constituição da República.

Infraconstitucionalmente, a proteção da privacidade se consubstancia na cláusula geral estabelecida no artigo 21 do Código Civil. Ainda, destaca-se que as previsões legislativas específicas para a proteção de dados são escassas. Tem-se, na Lei Federal nº 8.078/1990 - Código de Defesa do Consumidor, a regulamentação dos bancos de dados e cadastros de consumidores em único dispositivo, o artigo 43. Além disso, há a regulamentação do chamado cadastro positivo pela Lei Federal nº 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

3. UNIÃO EUROPEIA

A proteção dos dados no sistema normativo da União Europeia (UE) é tratada por meio de um sistema de regulamentos e diretivas, na qual é possível encontrar aspectos

pioneiros no regramento da matéria. Há registro de legislações, por exemplo, na Alemanha e Suécia desde a década de 1970. Portugal, em 1976, e, posteriormente, Espanha, em 1978, foram os primeiros países a elevar a proteção em nível constitucional, trazendo previsões expressas nas suas respectivas Cartas.

O Regulamento Geral sobre a Proteção de Dados, identificado como Regulamento 2016/679, e a Nova Diretiva (2016/680), trazem diretrizes para os países integrantes da UE. Ganham destaque também os Relatórios e Comunicações de acompanhamento da implantação e eficiência das normativas.

Cabe mencionar que desde o início de 2012 foi formada a Comissão Europeia para regulamentação sobre a proteção de dados pessoais. Entre os objetivos expostos há referência de que:

> La Comisión europea quiere modernizar la legislación europea de protección de datos para garantizar la intimidad de los consumidores y hacerla compatible con la libre circulación de datos en la UE . [...]
> Las empresas sólo estarán autorizadas a enviar información personal fuera de la UE a países con un nivel similar en sus sistemas de protección de datos. Se trata además de mejorar y simplificar los mecanismos de transferencia internacional de datos. [...]
> El objetivo de la nueva estrategia es consolidar un enfoque común en toda la UE. Las divergencias actuales no permiten determinar con nitidez la legislación aplicable en cada caso. Por eso es necesario armonizar las normas y reforzar el poder de las autoridades de protección de datos con el principio de cooperación y coordinación. (COMISIÓN EUROPEA, 2010).

Referidas premissas servem ao mesmo tempo como alerta à constante mutação e evolução da tecnologia e da forma como os dados podem ser armazenados e manipulados. É importante, ainda, considerar a facilidade do intercâmbio de informações e procurar meios para que essa circulação atenda a requisitos de segurança e preservação da privacidade.

A utilização dos recursos tecnológicos alterou significativamente a circulação, a forma de compartilhamento e o armazenamento de dados. A digitalização de documentos e o arquivamento de informações em bancos de dados digitais é cada vez mais significativo.

Nesse contexto, a proteção de dados pessoais nos sistemas jurídicos em geral necessita de uma análise mais criteriosa, principalmente no sistema jurídico brasileiro, no qual não se tem uma legislação específica acerca da proteção dos dados pessoais.

Ao contrário da legislação encontrada em países da Europa, não há no sistema jurídico brasileiro, por exemplo, uma autoridade responsável e independente, dedicada a

preservar o consentimento e o uso de dados pessoais mediante a supervisão do cumprimento das obrigações dos responsáveis pelo tratamento de dados, as quais possuem previsão específica (GALINDO, 2013, p. 136).

De acordo com a normativa europeia, em caso de descumprimento, qualquer cidadão pode reclamar à autoridade de proteção dos dados, a qual estará apta a instaurar procedimento administrativo e aplicar sanções ao responsável. Referida característica, conforme Galindo (2013, p. 137), é relevante, pois:

> ...se completó este cuadro de derechos y obligaciones con la atribución legal a la autoridad de protección de datos de su obligación de velar por el cumplimiento de las medidas conducentes a evitar la modificación de los datos personales por la utilización de las técnicas de seguridad de las TIC consideradas más adecuadas en cada momento.

A existência de autoridade responsável pela proteção dos dados, com atribuições claras e voltadas a não transgressão dos dados pessoais, afigura-se, portanto, um relevante mecanismo.

A autodeterminação informativa é um direito que orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico. "Concebido como um direito fundamental (...), o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações" (DONEDA, 2006, p. 196-197).

Em um julgamento (*BverfGE 65,1*) emblemático do Tribunal Constitucional Federal da Alemanha, de 15 de dezembro de 1983, averiguou-se a constitucionalidade da lei que ordenava o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho para fins estatísticos.

Segundo o Tribunal Constitucional Federal da Alemanha, em virtude das condições do moderno processamento de dados, o direito geral da personalidade contido no artigo 2 *I GG*, em conjugação com o artigo 1 *I GG*, passa a abranger a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, que somente podem ser utilizados, em princípio, com sua autorização. Essa norma consubstancia um direito geral à autodeterminação sobre a informação, que somente é restringível se houver

a contraposição de um interesse predominante da coletividade (SCHWABE, 2005, p. 233-235).

Na construção dessa norma concreta, o Tribunal Constitucional Federal da Alemanha considerou que o direito ao livre desenvolvimento da personalidade abrange o poder do indivíduo de decidir, por si próprio, quando, quais e em que limites os fatos pessoais serão revelados, poder que, diante da evolução tecnológica atinente ao processamento automático de dados, depende de uma proteção especialmente intensa (SCHWABE, 2005, p. 237).

A faculdade contemporânea e futura de armazenamento ilimitado, transmissão instantânea e consulta irrestrita de dados atentaria contra a autodeterminação individual, uma vez que não mais possibilitaria a determinação, com segurança, de quais informações sobre a sua pessoa são conhecidas, nem por quem são acessadas, inibindo substancialmente a liberdade de planejar ou decidir com autodeterminação (SCHWABE, 2005, p. 237).

Esse direito à autodeterminação informativa, porém, não é absoluto, mas restrito quanto às informações de interesse geral predominante, quer dizer, limitável excepcionalmente quando imprescindível para a consecução de um interesse público. Tais restrições exigem uma base constitucional que possibilite o conhecimento, pelo cidadão, de forma clara e reconhecível, dos pressupostos e da extensão das limitações, atendendo ao princípio da transparência do Estado de Direito (SCHWABE, 2005, p. 237-239).

O núcleo da autodeterminação informativa, enquanto relacionada ao aspecto básico do direito à intimidade, constitui-se na faculdade que a pessoa detém de escolher sobre a divulgação e a revelação de informações que diretamente a ela se referem.

Para Doneda (2006, p. 201) a terminologia mais adequada é tão somente "proteção de dados pessoais", pois estaria englobada tanto a problemática da privacidade quanto a da informação, que teria como ponto de referência os direitos da personalidade e estaria isenta de uma acepção patrimonialista ou contratual, ao mesmo tempo em que não remonta ao direito à liberdade em uma acepção demasiadamente ampla.

A crítica do jurista citado reside basicamente em três fatores. O primeiro é acerca da correta definição do que seja autodeterminação, pois em determinado sentido poderia dar ao indivíduo a oportunidade de controlar as informações que lhe digam respeito dentro de parâmetros quase ilimitados (DONEDA, 2006, p. 198).

Já para uma segunda leitura, em chave liberal, a autodeterminação concentrar-se-ia no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, afastando a matéria do âmbito dos direitos da personalidade (DONEDA, 2006, p. 198).

Por fim, outro fator seria a possibilidade de se ter a impressão de que as pessoas teriam um direito de propriedade sobre suas informações, o que as transportaria para o campo das situações patrimoniais (DONEDA, 2006, p. 198-199).

Outro aspecto a ser delimitado é a importância da existência de um órgão responsável pela proteção dos dados pessoais. Trata-se de órgão com diversas atribuições sociais, políticas e jurídicas, pois, como se observa em experiências europeias, além de fiscalizar, controlar e aplicar sanções à violação dos dados pessoais, cabe a promoção de ações educativas e de informação tanto para cidadãos quanto para órgãos públicos.

É preciso delimitar as atribuições, estrutura, composição e observar uma autonomia financeira e política a esse órgão. A vinculação a órgãos governamentais e ligados ao Poder Executivo não é desejável. Ainda, a dependência ao Poder Legislativo, Judiciário ou outros da estrutura jurídico-administrativa (Ministério Público, por exemplo) também podem comprometer a segurança dos dados, notadamente pelo interesse em determinadas demandas.

O novo órgão deve ter autonomia e meios efetivos de executar sanções aos infratores, além de organizar as políticas para a conscientização quanto à utilização e guarda de dados pessoais.

Ademais, sua composição deverá ser híbrida e seus integrantes oriundos de diversos segmentos sociais. Ao mesmo tempo em que é importante que se tenha um órgão com conhecimentos técnicos acerca da criação e manutenção de banco de dados é importante que haja uma interdisciplinaridade em seu Conselho administrativo.

Nesse sentido, referidos integrantes poderão advir de diferentes áreas do conhecimento contribuindo para uma melhor regulamentação da legislação protetiva e adequação à realidade das relações sociais e institucionais.

Ao falar sobre a independência de uma autoridade de proteção de dados, Doneda (2006, p. 393) afirma que referida característica pressupõe a presença de "mecanismos de nomeação de seus membros, geralmente limitando a discricionariedade na sua escolha (através, por exemplo, da exigência de determinada formação ou atuação profissional)", além

"da incompatibilidade de sua atuação com outras atividades, atuais ou mesmo pregressas (e também futuras [...]), além da limitação temporal de seu cargo" (DONEDA, 2006, p. 393).

Ainda, a independência pressupõe "a ausência de ingerência governamental sobre seus atos, que se pode obter situando tais órgãos fora de uma posição hierárquica em relação ao governo" (DONEDA, 2006, 393-394).

Além da especificidade referente à matéria e da função de velar pelo fiel cumprimento e respeito à lei, interpretando-a e aplicando-a, o ente independente deve ser dotado de poderes para inspecionar e aplicar sanções. É preciso que os responsáveis pelos arquivos mantenham referido órgão informado acerca das características de seu banco, além de, sendo o caso, quando requisitados, deem acesso aos dados que nele constam.

4. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

O PL 5276/2016 previa a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), a qual estava prevista nos arts. 55 a 57.

A referida Autoridade seria integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça.

Nos termos do PL 5276/2016, a ANPD deveria observar as disposições da Lei nº 9.986, de 18 de julho de 2000, a qual apresentada dispositivos acerca da gestão de recursos humanos das Agências Reguladoras e dá outras providências.

Ainda, foi prevista uma composição, por três membros, ao órgão máximo da Autoridade, o Conselho Diretor, compondo-a, ainda, pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação da Lei.

Foi dada a natureza de autarquia especial conferida à ANPD, caracterizando-a por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira.

Essas características apresentam elevado grau de relevância, eis que, ao menos em tese, atribuem mais liberdade para o cumprimento do dever de proteção dos dados e, conforme o caso, de sancionamento. Isso porque dão autonomia a seus agentes, concedendo-

lhes autonomia financeira, estabilidade no desempenho das funções e não a vinculando a ordem de outro órgão estatal ou privado.

Optara o legislador, por uma centralização da proteção de dados em um ente e seu principal auxiliar, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. A ANPD congregaria as competências de supervisão e consulta em matéria de proteção de dados, sendo responsável por assegurar que as instituições e órgãos do país respeitassem as obrigações estabelecidas.

Entre as atribuições da ANPF, havia estabelecido o art. 56 do PL 5276/2018:

> I – zelar pela proteção dos dados pessoais, nos termos da legislação;
> II – zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
> III – elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> V – atender petições de titular contra controlador;
> VI – disseminar o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança à população;
> 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, devendo esses padrões levar em consideração as 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 transnacional;
> X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos 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 e a natureza dos dados e os demais detalhes

> do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;
> XII – elaborar relatórios de gestão 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;
> 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 e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; e
> XVI – realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

Percebe-se um extenso rol de atribuições. O que não é estranho, tendo em vista que se vislumbra uma centralização em um ente forte e independente para a efetiva proteção de dados. E, para a concretização desse ideal, é premente a criação de uma órgão com qualificação técnica para lidar com a multidisciplinariedade da proteção de dados pessoais, que tenha competência normativa e propicie a ampla participação dos mais variados setores sociais. Soma-se a necessária transparência, imprescindível na configuração do Estado de Direito. Isso tudo além das características, já nominadas, da independência e autonomia financeira.

No que tange às receitas da ANPD, estabelecia o art. 57 do PL 5276/2016

> I – o produto da execução da sua dívida ativa;
> II – as dotações consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos;
> III – as doações, os legados, as subvenções e outros recursos que lhe forem destinados;
> IV – os valores auferidos na venda ou aluguel de bens móveis e imóveis de sua propriedade;
> V – os valores auferidos em aplicações no mercado financeiro das receitas previstas neste artigo;
> VI – o produto da cobrança de emolumentos por serviços prestados;

> VII – os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais;
> VIII – o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

A criação da ANPD viria ao encontro da regulamentação europeia de proteção de dados, sendo elemento relevante à preservação dos dados pessoais, evitando a modificação e trazendo subsídios para que sejam assegurados direitos fundamentais do cidadão, visando a não modificação e utilização indevida dos dados por meio de artifícios tecnológicos.

De acordo com a normativa europeia, em caso de descumprimento, qualquer cidadão pode reclamar à autoridade de proteção dos dados, a qual estará apta a instaurar procedimento administrativo e aplicar sanções ao responsável.

Atribuir por meio de uma lei a uma autoridade de proteção de dados, conforme Galindo Ayuda (2013, p. 137), é uma forma de se completar o quadro de direito e obrigações, dando-lhe a obrigação *de velar por el cumplimiento de las medidas conducentes a evitar la modificación de los datos personales por la utilización de las técnicas de seguridad de las TIC consideradas más adecuadas en cada momento*.

A existência de autoridade responsável pela proteção dos dados, com atribuições claras e voltadas a não transgressão dos dados pessoais afigura-se, portanto, um relevante mecanismo.

Não obstante a relevância do tema, a medida foi vetada pelo Presidente da República com argumento de discutível validade.

5. A MEDIDA PROVISÓRIA E A FRAGILIDADE DA AUTORIDADE INDEPENDENTE

No limiar do Governo Temer foi editada a Medida Provisória nº 869/2018, a qual altera a LGPD e cria a Autoridade de Proteção de Dados Pessoais. Entre as alterações está a aumento do período de *vacatio legis* para dois anos a partir da publicação.

A Autoridade Nacional de Proteção de Dados – ANPD, nos termos do art. 55-A, é órgão da Administração Pública Federal, integrante da Presidência da República, sendo-lhe assegurada, consoante o art. 55-B, assegurada autonomia técnica à ANPD.

No ponto em análise, não obstante a referência à autonomia técnica, fica evidenciada a dependência e a submissão da ANPD à chefia do Executivo Federal, retirando-se características primordiais a um órgão de proteção de dados.

A MP retira da redação original da LNPD as características da autonomia administrativa e ausência de subordinação hierárquica.

Foi estabelecido que a Autoridade é composta por um Conselho Diretor, órgão máximo de direção, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; e unidades administrativas e unidades especializadas à aplicação da lei.

O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente, nomeados pelo Presidente da República, ocupando cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5.

O mandato será de 4 anos, escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.

A remoção dos membros do Conselho Diretor ocorrerá apenas em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar instaurado pelo Presidente da República.

Não há, portanto, qualquer exigência de confirmação ou fiscalização por outro Poder da República acerca da nomeação a ser realizada, como o é, por exemplo, a exigência da sabatina pelo Senado no caso das Agências Reguladores convencionais.

Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente.

A estrutura regimental será estabelecida por ato do Presidente da República, sendo que, enquanto não definida, a ANPD receberá o apoio técnico e administrativo da Casa Civil para o exercício de suas atividades. É a esse Ministério, inclusive que terá atribuição de a instaurar o processo administrativo disciplinar contra os membros do Conselho Diretor.

Com relação ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, o texto da MP definiu que será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: seis do Poder Executivo federal; um do Senado Federal; um da Câmara dos Deputados; um do Conselho Nacional de Justiça; um do Conselho Nacional do Ministério Público; VI - um do Comitê Gestor da Internet no Brasil; quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; quatro de instituições científicas, tecnológicas e de inovação; e quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais.

Todos os representantes do Conselho serão designados pelo Presidente da República.

Imperioso salientar, ainda, que, nos termos da redação dada ao art. 55-A, a ANPD é criada sem aumento de despesa. Em outras palavras, significa dizer que se retira da Autoridade de Proteção a imprescindível autonomia financeira. A referida característica é essencial na consecução de seus objetivos de proteger de forma eficaz os dados pessoais em um mundo em que o cidadão está vulnerável e a sua privacidade comprometida.

A vinculação do órgão à Administração Direta, vinculando-a à Presidência da República compromete igualmente a execução dos objetivos da Autoridade, trazendo subordinação hierárquica e ausência de autonomia administrativa. Essas características estavam presentes na lei de proteção de dados e a sua retirada reduz substancialmente a eficácia e efetividade da Autoridade. Como observado, são elementos indissociáveis a uma atuação qualitativa do ente.

Impende, também, aduzir a insegurança que uma MP traz à temática. Para exemplificar, até o último dia 03 de abril, a comissão mista que analisa a MP 869/18 ainda não havia votado seu plano de trabalho. Até o momento, já foram apresentadas 176 emendas ao texto (CÂMARA DOS DEPUTADOS, 2019).

Por meio do Ato Declaratório n. 17, de 27/03/19, do Presidente da Mesa do Congresso Nacional, foi prorrogada a vigência da Medida Provisória nº 869 pelo período de sessenta dias, consoante publicação no Diário Oficial da União de de 28/03/19, Seção 1, Página 3.

6. CONCLUSÃO

O sistema jurídico de proteção dos dados pessoais deve ser constituído de uma estrutura sólida que dê transparência e que estabeleça um sistema de identificação e armazenamento de dados com salvaguardas. É necessária uma definição clara acerca de quem controla, quem fiscaliza, quem é responsável e a forma como os dados podem ser compartilhados.

Atualmente é percebido que recrudescimento de iniciativas governamentais que, em nome de economia e simplificação da atividade administrativa, promovem a abertura de bases de dados do governo federal brasileiro, suas autarquias e entidades controladas, sem as necessárias salvaguardas referentes à proteção da privacidade e dos dados pessoais.

No presente estudo foi verificado que o sistema jurídico brasileiro não apresenta as salvaguardas necessárias à proteção da privacidade, confirmando-se a hipótese inicial de que a Medida Provisória nº 869 compromete a atuação efetiva e eficaz da Autoridade de Proteção de Dados brasileira.

As características trazidas à ANPD não garantem proteção adequada e se torna temerária na medida em que coloca em risco a garantia individual de proteção da privacidade, eis retira elementos imprescindíveis à operacionalização do seu fim, entre eles, a autonomia administrativa e a não subordinação hierárquica.

Entre os elementos destacados no artigo, revela-se ínsito a uma Autoridade de Proteção de Dados as garantias para que possa desempenhar com independência sua missão institucional. Elas devem assegurar que pareceres técnicos sejam emitidos sem a influência de posições ideológicas ou político-partidárias. Ademais, não poderá estar submetida a ameaças ou influências externas, muito menos do titular da chefia de um dos poderes da República.

É preciso que a composição seja exclusiva por profissionais habilitados e atualizados com a evolução cada vez mais rápida da tecnologia. A composição deve ser híbrida e multidisciplinar, especializado e sem subordinação a órgãos estatais e privados. As demandas, em especial com a aplicação das técnicas de inteligência artificial, aprendizado de máquina, consubstanciam grau de complexidade elevado, exigindo conhecimento e independência na execução das atividades.

De pouco adianta ao Brasil ter uma lei de proteção de dados pessoais, mas não ter uma autoridade com as características elencadas. O reconhecimento de países que possuem tal

sistema ficará prejudicado, afetando as relações com esses países, eis que a tema tem sido objeto de significativa preocupação, principalmente nos países da União Europeia.

O uso indiscriminado dos dados pessoais, além de vulnerar direito fundamental, facilita o controle e monitoramento dos cidadãos.

Os dados e informações pessoais devem ter um controle mais amplo pelo próprio indivíduo, o qual necessita ter acesso às informações armazenadas nos bancos de dados a seu respeito, podendo exigir a sua retirada ou alteração e atualização. Busca-se, em última análise, a correção dos dados, conhecimento pelo indivíduo acerca da existência de cadastro e do que consta a seu respeito.

7. REFERÊNCIAS

BRASIL. Congresso Nacional. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 07 set. 2018.

BRASIL. Congresso Nacional. **Medida Provisória nº 869**, de 27 de dezembro de 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 04 abr. 2019.

CÂMARA DOS DEPUTADOS. **Comissão de MP que muda Lei de Proteção de Dados Pessoais vota plano de trabalho**. 2019. Disponível em <https://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/574446-COMISSAO-DE-MP-QUE-MUDA-LEI-DE-PROTECAO-DE-DADOS-PESSOAIS-VOTA-PLANO-DE-TRABALHO.html>. Acesso em: 03 abr. 2019.

COMISIÓN EUROPEA. **Estrategia de la ue para la protección de datos en internet**. 2010. Disponível em <http://ec.europa.eu/spain/actualidad-y-prensa/noticias/internet-y-sociedad-de-la-informacion/proteccion-datos-internet-ue_es.htm>. Acesso em: 23 set. 2015.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GALINDO AYUDA, Fernando. Seguridad y sociedad del conocimiento. In: GALINDO, Fernando (ed.). **El derecho de la sociedad en red**. Lefis Series, 14. Zaragoza: Prensas de la Universidad de Zaragoza, 2013. p. 129-154.

LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHWABE, Jürgen. **50 anos de jurisprudência do tribunal federal constitucional alemão**. Traduzido por Beatriz Hennig et all. Montevidéu: Fundacion Konrad-Adenauer, 2005.