Resolução da ANPD - aplicação da LGPD para startups e pequenas empresas

CONSULTA PÚBLICA ANPD: TOMADA DE SUBSÍDIOS

ASSUNTO: Tomada de subsídios para regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

Autores

Paola Cantarini

Willis S. Guerra Filho

Zilda A. Gonçalves de Sousa

Marcio Pugliesi

Jhésica Baccari

INTRODUÇÃO

Comentários Gerais

A regulamentação do art. 55, XVIII da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), no que se refere a sua aplicação para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos visa facilitar a adequação destes agentes à LGDP, diante da baixa maturidade e cultura de proteção de dados dos agentes de pequeno porte, e de modo geral, no Brasil. De partida, vale destacar que as vultosas multas previstas na LDGP poderiam inviabilizar a existência de tais agentes, reduzindo o potencial de inovação e estímulo econômico no país, com prejuízo para o próprio desenvolvimento do país.

O art. 55, inc. XVIII da LGDP prevê que a ANDP poderá editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se

autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei (incluído pela Lei nº 13.853, de 2019). Pela redação supra citada, percebe-se que a regulamentação a cargo da ANPD se limitaria a facilitar a adoção de procedimentos e cumprimento de obrigações constantes da LGPD, não abrangendo, portanto, a exclusão ou limitação de obrigações, como em alguns pontos parece ser o objetivo da presente proposta legislativa.

Outrossim, enquanto a LGPD apenas traz a possibilidade de flexibilização de cumprimento de suas normas para as pessoas jurídicas indicadas de forma expressa e taxativa (microempresas, empresas de pequeno porte e startups), a nova proposta regulamentadora vai além e abrange agentes não previstos pela LGPD, ampliando seu objeto, qual seja, de mera regulamentação, para inovação em aspectos significativos, donde é forçoso admitir que não se está apenas regulamentando mas legislando, ao abranger entidades sem fins lucrativos, como igrejas, extrapolando assim a abrangência e os limites legais do poder de regulamentar a LGPD. A norma regulamentadora da lavra da ANPD poderá apenas complementar ou explicitar as disposições da LGPD e facilitar com isso sua efetiva aplicação, não podendo, a pretexto de estar regulamentando, pretender alterar a LGPD.

A abordagem de risquificação, trazendo já de forma expressa no texto legislativo os diversos graus de riscos, e exemplos de atividades consideradas como de alto risco, moderado e baixo risco seria uma abordagem mais prudente, a fim de se evitar imprecisões, dúvidas, antinomias, contribuindo para a segurança jurídica, a exemplo do que foi adotado pela Comissão Europeia ao propor a criação de regras padrão, de adesão voluntária, com o estabelecimento de requisitos obrigatórios baseados no risco, para aplicações de alto risco. Segundo o documento denominado “White Paper on Artificial Intelligence”, de 19/02/2020, é recomendada a elaboração de uma separação, para fins regulatórios, entre as tecnologias de inteligência artificial “comuns” e as que oferecem um alto risco, devendo ser observadas algumas condições-chave, com destaque para a robustez, a precisão e a supervisão humana, devendo ainda ser garantidas a privacidade e a proteção de dados. Da mesma forma, é o que se verifica na Recomendação do Conselho da Europa de 2010, apontando para a necessidade da observância do princípio da precaução, um princípio explícito de regulação do risco, bem como na nova proposta da Comissão Europeia de Regulamentação da IA, de 21/04/2021.

Com a entrada em vigor da Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), houve um grande marco para o Brasil – quando da possibilidade da sua entrada no rol dos mais de 100 países com legislações específicas sobre a temática “Privacidade e Proteção de Dados Pessoais”, beneficiando a entrada do Brasil no comércio internacional e nas relações comerciais com mercados que já carregam a primazia de exigências de cumprimento às legislações voltadas para a temática e necessárias ao fluxo transfronteiriço de dados

pessoais. Além disto, com a aprovação da LGPD, os titulares dos dados pessoais passam a ter efetivamente o controle sobre os seus dados pessoais e sobre o tratamento que porventura, vier a ser realizado.

Assim, há a clara preocupação da legislação em garantir a proteção dos direitos e garantias fundamentais dos titulares dos dados pessoais, frente aos desafios tecnológicos, econômicos e políticos atuais, decorrentes da Era do *Big Data,* da rápida evolução tecnológica e da globalização.

Por isso, a LGPD estabelece disposições como, requisitos para o tratamento dos dados pessoais e dados pessoais sensíveis, direitos dos titulares, tratamento de dados pessoais pelo Poder Público, regras para transferência internacional de dados pessoais, definição de conceitos importantes, exigência segurança, sigilo, regras de boas práticas e governança, quando do tratamento dos dados pessoais, além, de disposições relacionadas à Autoridade e ao Conselho Nacional de Proteção de Dados Pessoais (ANPD), além de capítulo destinado à fiscalização e sanções administrativas.

NORMA DE APLICAÇÃO DA LGPD PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

Dentre os diversos desafios que se colocam em tela para implementação da LGPD, percebe-se que é essencial adequar o texto normativo à realidade das micro e pequenas empresas, a fim de se evitar que a burocratização possa inviabilizar os pequenos negócios.

Por isso, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) lançou Consulta Pública para coletar subsídios sobre a regulamentação da aplicação da Lei Geral de Proteção de Dados para microempresas e empresas de pequeno porte, e, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

COMENTÁRIOS ARTIGO POR ARTIGO

Artigo 2º

Por outro lado, **a opção regulatória utilizada ao adotar o critério de porte do agente,** independente do volume de dados pessoais objeto de tratamento, e independente do tipo de dados pessoais tratados, ordinários ou sensíveis, ou de crianças e adolescentes, talvez não seja a melhor opção, no sentido de atrelar tal categorização a uma valoração de grau de risco. Isto é, pelo simples fato de se enquadrar como uma startup e pequena empresa, não implica *ipso facto,* em um volume baixo de tratamento de dados. Uma pequena empresa

ou startup poderá efetuar tratamento de dados de milhões de pessoas, compartilhar com parceiros econômicos, portanto, o critério legal não poderia ser o número de colaboradores ou faturamento e sim o volume de dados pessoais tratados, a probabilidade de um maior grau de risco, a depender do tipo de atividade praticada com os dados pessoais, e a depender do tipo de dado pessoal tratado, se dado sensível, se dado de crianças e adolescentes, quando teríamos um maior grau de risco, já que maior o potencial de danos, de discriminação e uma maior vulnerabilidade.

Sabe-se que quando se trata de direitos fundamentais, como é o caso do direito à autodeterminação informativa atrelada ao direito de proteção de dados, pelo titular de dados, que a interpretação vinculada a uma análise econômica ou utilitarista não seria a melhor opção, visando maior proteção de direitos fundamentais. Neste sentido, tem-se o reconhecimento do direito fundamental à proteção de dados pelo art. 8 da Carta de Direitos Fundamentais da União Europeia, proclamada pelo Parlamento Europeu, pelo Conselho da União Europeia e pela Comissão Europeia em 7.12.2000.

Verifica-se que o objetivo da minuta da Resolução submetida à consulta pública tenta, sem conseguir na verdade, aplicar o princípio da proporcionalidade, ao trazer uma certa forma de ponderação, de um lado, visando a proteção dos direitos dos titulares de dados, e de outro, buscando um equilíbrio em tal relação jurídica, reduzindo a carga de obrigações para os agentes mencionados, de modo a não impedir a inovação e o desenvolvimento econômico. Ora, uma aplicação correta de tal princípio, como temos defendido doutrinariamente desde textos que introduziram o tema no País, requer a observação de limites ao se fazer recuar interesses respaldados em direitos fundamentais, ainda que em benefício de outros, com igual respaldo, sendo este limite estabelecido pelo respeito incondicional à dignidade humana, o que no caso em apreço requer maior cuidado com os mais vulneráveis, para além de considerações de ordem econômica.

Ressalte-se, assim, a importância de se estudar a proteção de dados como direito fundamental, não apenas como direito humano, de abrangência mais ampla, internacional, ou como um direito de personalidade autônomo, de abrangência mais restrita, privatista, estabelecendo-se parâmetros constitucionais para o tratamento da matéria, e daí a importância do estudo da Teoria dos Direitos Fundamentais, permitindo a adequada compreensão dos direitos fundamentais e, em relação a eles, dos princípios da razoabilidade e da proporcionalidade, diversos em conceito, origem e função, previstos tanto na jurisprudência mais abalizada, como na própria LGPD – Lei Geral de Proteção de Dados, Lei nº 13.709/2018, ainda que sem nomeá-los, em seu art. 6º, incs. I, II e III.

Tal temática envolta à presente consulta pública, portanto, demanda uma abordagem constitucional, que resulte em contribuição a uma Teoria Fundamental do Direito Digital, enquanto teoria jurídica, desenvolvida à luz do Direito Constitucional, dos princípios constitucionais, da nova hermenêutica constitucional, aplicando-se a ponderação de forma correta no caso, por meio da aplicação do princípio da proporcionalidade, possibilitando, destarte, de um lado, a manutenção e incremento da inovação e livre desenvolvimento da atividade econômica, e de outro, a proteção adequada do titular dos dados.

Portanto, se faz necessário para sua compreensão o estudo da Teoria dos Direitos Fundamentais, com a distinção de normas jurídicas que são regras e daquelas que são princípios, a fim de compreender de forma adequada, por exemplo, como se daria a ponderação, no caso de colisões de normas de direitos fundamentais relacionadas à proteção de dados, por meio do princípio da proporcionalidade.

Traz a ponderação a necessidade de observância de todo um procedimento racional, objetivo, com a aplicação dos três subprincípios da proporcionalidade, necessidade, adequação e proporcionalidade em sentido estrito, justamente a fim de se evitar decisões arbitrárias, subjetivistas, contribuindo assim para a efetividade do Direito e sua maior racionalidade. Há necessidade de análise, portanto, dos subprincípios da adequação, de um lado, e de outro o da exigibilidade, necessidade ou indispensabilidade (*Erforderlichkeit*), os quais determinam, respectivamente, que o meio escolhido se preste a atingir o fim colimado, mostrando-se assim “adequado”, meio este que também deve se mostrar “exigível”, o que significa que não há outro igualmente eficaz e menos danoso aos direitos fundamentais envolvidos, considerados conjuntamente.

Em suma, pelo subprincípio da adequação a medida restritiva em causa deve ser apta a realizar o fim visado. Pelo subprincípio da exigibilidade, da necessidade, da indispensabilidade, ou máxima do meio mais suave (*Gebot des mildesten Mittels* ou *Erforderlichkeit*), entre todos os meios idôneos disponíveis e igualmente aptos a perseguir o fim visado, deve-se escolher o que produza efeitos menos restritivos a direitos e interesses fundamentais concernidos. A adequação e a exigibilidade determinam, respectivamente, que, dentro do faticamente possível, o meio escolhido se preste para atingir o fim estabelecido, mostrando-se, assim, “adequado”, e, além disso, para ser admitido, não haja outro menos ofensivo aos direitos e princípios fundamentais colidentes, eis que esse meio deve se mostrar “exigível” - o que significa não haver outro igualmente eficaz a se indicar e menos danoso a direitos fundamentais. Por fim, o subprincípio da proporcionalidade em sentido estrito se traduz deonticamente em proibição de excesso a fulminar, portanto, o núcleo essencial intangível e razão de ser de todos os princípios, direitos e garantias fundamentais de Estado Democrático de Direito: a dignidade humana.

Referido subprincípio determina que se estabeleça uma correspondência entre o fim a ser alcançado por uma disposição normativa e o meio empregado, que seja juridicamente a melhor possível. Isso significa, acima de tudo, que não se fira o "conteúdo essencial" (*Wesensgehalt*) de direito fundamental, com o desrespeito intolerável da dignidade humana, bem como que, mesmo havendo desvantagens para o interesse de pessoas, individual ou coletivamente consideradas, resultante da disposição normativa em apreço, as vantagens que traz para interesses de outra ordem que não aquela meramente econômica superam aquelas desvantagens. O princípio da proporcionalidade como um todo, portanto, promove, sem jamais aviltar, a dignidade humana e constitui um meio seguro para o julgamento de casos envolvendo conflitos entre direitos humanos e fundamentais.

Trazendo para a discussão do tema, o Considerando 13 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), percebe-se que haverá tratamento diferenciado às micro, pequenas e médias empresas, ou seja, há de se reservar às empresas de pequeno porte obrigações e procedimentos simplificados, levando em consideração a noção de micro, pequenas e médias empresas que deve inspirar-se do **artigo 2.o do anexo da Recomendação 2003/361/CE da Comissão.**

Assim, sugere-se como elemento para concessão de procedimentos simplificados às empresas de pequeno porte:

- **Natureza, Volume e Tipo de Dados Pessoais Tratados:**

  Quanto mais sensíveis os dados pessoais tratados (e sendo estes o "cool business" da organização), quanto maior o volume de dados pessoais tratados e levando em consideração a vulnerabilidade da classe de titulares afetados (crianças, adolescentes e idosos)– **há de se exigir medidas adicionais 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, nos moldes do art. 46, da LGPD**.

- **Definição dos Agentes de Tratamento:**

  Um dos elementos que aparece na legislação brasileira serve de indicativo para se diferenciar **agentes de pequeno porte de outros agentes quanto ao tratamento de dados pessoais está na exceção da exigência de nomeação do Encarregado pelo Tratamento dos Dados Pessoais (DPO).**

Sugere-se que critérios sólidos sejam levados em consideração para a definição de agentes de tratamento, como: a) Risco da Atividade (Cool Business); b) Definição de empresas de pequeno porte deve-se levar em conta o número de funcionários ou da receita bruta da empresa e tamanho da organização; c) Os critérios para escalonamento e classificação dos riscos devem levar em conta o processamento em grande escala e categorização dos dados.

- **Aplicação de sanções administrativas pautadas na análise dos riscos da atividade de tratamento de dados pessoais**

  Sugere-se que a aplicação de sanções considere e seja adequada ao grau do risco que as empresas representam quando do tratamento dos dados pessoais, a natureza da atividade e a finalidade, a fim de não onerar excessivamente e inviabilizar o negócio das micro, pequenas e médias empresas, levando em consideração o importante balanceamento e equilíbrio entre a garantia dos direitos fundamentais da privacidade e proteção de dados pessoais dos titulares, mas tão importante quanto, garantir o fomento ao desenvolvimento socioeconômico.

- **Garantir o livre desenvolvimento econômico- tecnológico e da inovação**

  De acordo com o **art. 2º, incisos V e VI, da LGPD**, a disciplina da proteção de dados pessoais tem como fundamentos: **a) o desenvolvimento econômico e tecnológico e a inovação; e b) a livre iniciativa, a livre concorrência e a defesa do consumidor.**

  Por isso, as normas de privacidade e proteção de dados pessoais devem garantir que os direitos fundamentais e o livre desenvolvimento da personalidade da pessoa natural sejam assegurados, ao lado dos fundamentos do desenvolvimento econômico e tecnológico e a inovação; e da livre iniciativa, a livre concorrência e a defesa do consumidor.

- **Segurança jurídica como fomento às atividades econômicas de mirco-empresas e empresas de pequeno porte**

  Deve-se assegurar um nível adequado de proteção de dados pessoais coerente, elevado e homogêneo, que seja apto a garantir a segurança jurídica às atividades de tratamento de dados pessoais – além eliminar obstáculos ao desenvolvimento dos pequenos negócios.

- **Elaboração de Regras Claras direcionadas às micro-empresas e empresas de pequeno porte**

Devem ser criadas regras claras com de etapas definidas e objetivas para adequação das micro-empresas e empresas de pequeno porte à Lei Geral de Proteção de Dados Pessoais (LGPD).

Artigo 2º, IV

IV - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

Emenda - Profº Dr. Márcio Pugliesi e Profª Jhesica Baccari: agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups, pessoas jurídicas sem fins lucrativos, **sociedade individual de advocacia e advogados autônomos** que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

Artigo 3º, *caput*

Outro ponto a ser destacado é a definição de alto risco, consoante *caput* do artigo 3º, pois não está claro se há apenas uma exemplificação ou uma tipificação taxativa, sem possibilidade de se aplicar analogia ou ser ampliada a lista de atividades citadas como consideradas de alto risco.

A regulamentação poderia trazer maiores informações acerca das atividades de alto risco, trazendo uma lista mais ampla de atividades. Poderia ser mencionado a título de exemplo o Considerando 75 do GDPR, trazendo alguns parâmetros para a análise da gravidade e natureza dos possíveis riscos aos direitos e às liberdades individuais dos titulares, *verbis*:

> "(...) poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; (...)".

Dados de grupos vulneráveis também é uma redação muito abrangente e não traz uma objetividade e clareza, sendo um conceito aberto, objeto de diversas interpretações, de quais grupos se enquadrariam como vulneráveis, podendo dar ensejo à dúvidas quanto a tal inclusão. Por conseguinte, a melhor

técnica legislativa deveria literalmente afirmar quais os grupos vulneráveis, explicitamente.

O ***caput* artigo** fala em dispensa e flexibilização das obrigações que são previstas na resolução. A ANPD não pode dispensar uma obrigação legal. Pode criar formas e mecanismos para segmentos específicos cumprirem a obrigação legal, mas não simplesmente dispensar. Se o fizer, poderá ser questionada judicialmente por contrariar norma legal.

O ***caput*** do artigo fala que não serão abarcados pela resolução (de dispensa e flexibilização das regras legais) os agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares. Como a resolução refere-se também a startups, pessoas jurídicas sem fins lucrativos, microempresas e empresas de pequeno porte e zonas acessíveis ao público, é importante que todas essas definições sejam incluídas como exceção à aplicação da resolução quando realizarem o tipo de tratamento especificado nesse artigo. Não faria sentido ficarem de fora, seria contrário a toda a lógica do texto.

Outro ponto absolutamente relevante é trocar o ´e´ por um ´**ou**´ quando o artigo fala em ´tratamento de alto risco e em larga escala para os titulares´. Isso porque o tratamento de alto risco, por si só, já demanda a necessidade de não haver flexibilização de qualquer tipo. O mesmo pode-se dizer daquele que é feito em larga escala. Em nenhuma das duas hipóteses, ainda que encontradas separadamente, poderia ter-se qualquer flexibilização das regras da LGPD. Ao revés, para esses dois casos, ainda que o tratamento de dados seja feito pelas pessoas indicadas no art.2º, é fundamental que a ANPD exija o rigor do cumprimento da lei, em razão da magnitude dos riscos potenciais envolvidos.

Artigo 3º, parágrafo 1º, I e II

Embora a própria normativa preveja duas situações em que tais dispensas e flexibilizações não poderão ocorrer, consoante *caput* do artigo 3º: I) quando o tratamento de dados for considerado de alto risco para os titulares, (parágrafo 1º), e II) quando o tratamento for considerado de larga escala (parágrafo 2º), há algumas falhas legislativas, senão vejamos.

O tratamento de **dados pessoais sensíveis (parágrafo 1º, I)** é considerado como sendo de alto risco, contudo, o critério adotado pela LGDP no tocante à definição em uma lista taxativa dos dados pessoais sensíveis, não seria a melhor interpretação, como adiante será demonstrado.

Por exemplo, embora a imagem de uma pessoa não se enquadre tecnicamente no conceito de dado pessoal sensível, como sendo um dado biométrico, segundo parte da doutrina, seguindo-se, inclusive, o entendimento consolidado de acordo com o GDPR, trata-se de uma interpretação literal e gramatical. Segundo o GDPR (RGPD, art.º 9.º n.º 1), o reconhecimento facial é caracterizado como produtor de “dados biométricos”, os quais estão entre as “categorias especiais de dados” (dados sensíveis), isto é, os “dados pessoais

resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular [natural] que permitam ou confirmem a identificação única dessa pessoa singular [natural], nomeadamente imagens faciais ou dados dactiloscópicos" (art.º 4.º 14), indo além da videovigilância / videomonitoramento. Ou seja, o tratamento de fotografias, a princípio, não deverá ser considerado sistematicamente um tratamento de categoria especial de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular através de algoritmos de IA.

Contudo, o conceito de dados pessoais sensíveis abarca outras hipóteses não previstas no texto da lei, considerando-se o potencial lesivo do tratamento de tal dado em questão, interpretando-se o artigo 5, inc. II da LGPD como não trazendo um rol taxativo, mas exemplificativo. O caso concreto deverá ser analisado, pois poderá ocorrer que diante de um dado pessoal ordinário seja possível auferir-se um dado pessoal sensível como no caso de uma fotografia que deixe clara a opção religiosa da pessoa, ou dados sobre sua origem racial ou étnica. Este entendimento se coaduna com a proteção adequada dos direitos fundamentais envolvidos (MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Revista do Advogado n. 144, 2019, pp. 47-53).

O **parágrafo 1º, inciso I** classifica de alto risco para os titulares o tratamento de dados pessoais sensíveis ou de grupos vulneráveis, incluindo crianças e adolescentes e idosos. Esse inciso encontra respaldo em todo o ordenamento jurídico positivado no país. Dados sensíveis são dados que receberam do legislador infraconstitucional maior atenção e maiores proteções. Até por isso possui bases legais de tratamento diferenciadas (art. 11, LGPD) em relação às gerais (art. 7, LGPD). São dados que podem causar, potencialmente, riscos mais graves aos titulares, como, por exemplo, de discriminação. Da mesma forma, o legislador também diferenciou o tratamento de dados pessoais de crianças e adolescentes, prevendo que o tratamento de seus dados pessoais única e exclusivamente só poderá acontecer com base no seu melhor interesse (art. 14, LGPD).

Com efeito, tanto o art. 11, quanto o art. 14, LGPD possuem o mesmo grau de exigência legal em relação ao consentimento, que, em ambos os casos, é igual e mais qualificado em relação ao consentimento previsto para os demais casos. Daí, a se entender, até mesmo, que os dados pessoais de crianças e adolescentes, para fins da LGPD, podem ser considerados dados pessoais sensíveis por conta dos potenciais riscos que envolve, para pessoas que, por sua condição peculiar de desenvolvimento biológico e psicossocial, estão em formação das suas capacidades físicas, cognitivas e emocionais.

Ainda que assim não se entenda, o que se admite para argumentar, pode-se dizer que dados pessoais de crianças podem ser equiparados a dados sensíveis, em função da necessidade de sua maior proteção, motivo pelo qual, além da base legal do consentimento, prevista no *caput* do art. 14, LGPD, as

bases legais do art. 11, LGPD também se aplicam às crianças – mas não as bases legais do art. 7º, LGPD.

Ademais, independentemente de se concordar com tais entendimentos, o que, mais uma vez, admite-se para fins de argumentação, é imprescindível notar que às crianças e aos adolescentes o legislador constitucional garantiu a máxima proteção, alçando tais entes sociais à maior preocupação da nação, quando determinou que seus direitos fundamentais devem ser garantidos com absoluta prioridade (art. 227, CF). Em toda a Constituição Federal, nenhum outro ente da sociedade ganhou tamanha proteção.

Aliás, as palavras ´absoluta´ e ´prioridade´ não se encontram juntas em nenhum outro artigo constitucional. Vale, também, ressaltar, que esse mesmo dispositivo constitucional também determinou que a responsabilidade pelo cuidado, proteção e promoção dos direitos fundamentais de crianças e adolescentes deve ser compartilhada entre famílias, Estado e sociedade (na qual incluem-se as empresas e os agentes abarcados pela proposta de resolução em comento). Isso significa que, mesmo que não se entenda serem dados pessoais de crianças e adolescentes dados pessoais sensíveis ou equiparados a dados pessoais sensíveis, fato é que esse grupo de pessoas já foi considerado, pela Constituição Federal, um grupo vulnerável a demandar mais proteção e atenção. Motivo pelo qual em absoluta correção a proposta apresentada pela ANDP para o art. 3º, I da minuta de resolução. Da mesma forma e no mesmo sentido, a inclusão do grupo de idosos como um grupo vulnerável, que são considerados absoluta prioridade pelo art. 3º, Estatuto do Idoso (Lei 10.741/2003).

Artigo 3º, parágrafo 1º, III

Ao afirmar como de alto risco o parágrafo 1º, "**III - uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade",** a proposta legislativa peca por excesso, já que em tese qualquer tratamento de dados possui tal potencial danoso. Falta objetividade em tal dispositivo legal, além de ser extremamente abrangente.

Artigo 3º, parágrafo 1º, IV

Também ao mencionar como sendo de alto risco o **parágrafo 1º, "IV - tratamento automatizado de dados pessoais que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade",** a proposta não inclui, por exemplo, decisões automatizadas que produzem decisões judiciais, as quais seriam tão ou mais relevantes que as definições de perfis.

Por sua vez, traz insegurança jurídica ao não descrever de forma concreta qual o número significativo de titulares possivelmente afetados ou o número

relativo ao volume de dados envolvidos, duração, frequência e extensão geográfica do tratamento, ao considerar o tratamento de dados como de larga escala, trazendo insegurança jurídica. Deveria haver uma definição mais precisa de tais termos.

Artigo 3º, parágrafo 2º - proposta

O tratamento de dados será caracterizado como de larga escala quando abranger **a partir de 50 usuários e/ou 100GB de armazenamento de dados pessoais**, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado

Artigo 4º *caput*

Art. 4º - Caberá ao agente de tratamento de pequeno porte avaliar e, quando solicitado pela ANPD, **comprovar por meio do Relatório de Impacto à Proteção de Dados Pessoais** o seu enquadramento nas disposições do art. 2º e do art. 3º.

Artigo 4º, parágrafo único

A ANPD poderá alterar o enquadramento apresentado pelo agente de tratamento de pequeno porte em sua atividade fiscalizatória**, mediante a avaliação do impacto das operações de tratamento.**

Artigo 6º, §1º

No caso em questão da consulta pública temos de um lado o direito à proteção de dados, como direito fundamental, e de outro, o livre desenvolvimento da atividade econômica. Por conseguinte, jamais poderia uma regulamentação **prever o não respeito pelos agentes indicados de alguns dos direitos básicos dos titulares de dados**, como ao dispor no seu **artigo 6º, §1º que "os agentes de tratamento de pequeno porte estão dispensados de conferir portabilidade dos dados do titular a outro fornecedor de serviço ou produto, nos termos do inciso V do art. 18 da LGPD",** pois isso afrontaria o princípio da proporcionalidade, já que há outras formas menos ofensivas a tais direitos que poderiam ser adotadas, como, por exemplo, dispor de um maior prazo para o seu cumprimento.

Artigo 7º caput e parágrafo único

> Art. 7º Os agentes de tratamento de pequeno porte ficam dispensados de fornecer a declaração clara e completa de que trata o art. 19, inciso II, da LGPD.
>
> **Parágrafo Único: o titular de dados poderá exercer o seu direito de confirmação de existência ou de acesso aos seus dados pessoais em formato simplificado no prazo de até quinze dias, contados da data do requerimento do titular.**

Art. 10 *caput* e parágrafo único

Ao prever em seu **artigo 10 *caput*** que **"os agentes de tratamento de pequeno porte ficam dispensados da obrigação de manutenção de registros das operações de tratamento de dados pessoais constante do art. 37 da LGPD,** e após no seu parágrafo único que **a ANPD fornecerá modelos para o registro voluntário e simplificado das atividades de tratamento,** parece contradizer o princípio da transparência e da prestação de contas, aos quais devem respeito todos os agentes, mesmo os beneficiados com as flexibilizações da presente regulamentação. Melhor seria, manter tal obrigatoriedade, mas possibilitando que seja feita de forma simplificada, mensurando e explicitanto alguns parâmetros necessários e requisitos indispensáveis como conteúdo de tal registro simplificado.

Artigo 10 sugestão de inclusão do parágrafo 2º

> **Parágrafo segundo. Fica incumbido aos prestadores de serviços aos agentes de tratamento de pequeno porte que tenham contratados serviços de tecnologia para cadastro e armazenamento de dados pessoais o registro e manutenção das operações de tratamento de dados pessoais, como por exemplo o log de registro contendo nome de usuário, endereço de IP, caminho percorrido, ações movidas no sistema, dia e horário de acesso, no mínimo.**

Artigo 11

O artigo 11 prevê que "**os agentes de tratamento de pequeno porte podem apresentar o relatório de impacto à proteção de dados pessoais de forma simplificada quando for exigido, nos termos da resolução específica".**

Quanto à elaboração do **Relatório de Impacto (art. 38, LGPD), pois embora não dispense tais agentes de tratamento em questão de sua elaboração, aponta a Resolução que poderá ser apresentado de forma simplificada** quando exigido pela ANPD. Neste ponto, é falha ao considerar a elaboração de tal importante documento obrigatória apenas após a requisição pela ANPD, tornando até mesmo sem sentido a elaboração de tal documento, que deverá necessariamente ser elaborado *antes do início do tratamento de dados*. Isto porque tal momento será determinante para a empresa pensar acerca do risco da atividade de tratamento de dados, com vista a tomar as medidas de segurança aptas a minorar tais riscos às liberdades e direitos fundamentais dos titulares, e deverá contemplar todo o projeto e "iter" do tratamento de dados.

Isto se tornaria impossível ou seria de todo farsesca sua elaboração, se apenas fosse elaborado após a solicitação pela ANPD. Exigir a elaboração de tal documento apenas após solicitação pela ANPD seria, portanto, um contrassenso, violando o princípio da razoabilidade e sua proibição do absurdo, do despropósito, já que necessariamente deverá ser elaborado antes do início do tratamento, com uma visão completa de todo o ciclo de vida dos dados, para que faça sentido e se justifique sua razão de ser.

Por derradeiro, melhor seria se a regulamentação trouxesse algum parâmetro mínimo para a elaboração simplificada de tal documento, a exemplo do art. 35 do GDPR, que traz uma lista de requisitos mínimos obrigatórios a serem preenchidos pelo relatório de impacto (não simplificado), e a exemplo de várias ANPDs de diversos países, como o Information Comissioner Officer (ICO) do Reino Unido, que trazem modelos de estrutura do Relatório.

Artigo 12 - sugestão de inclusão do parágrafo único

> **Parágrafo único. Fica vedada a dispensa da comunicação de incidente de segurança aos agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares.**

Artigo 13 *caput*

O **art. 13 *caput*** desobriga os agentes de tratamento de pequeno porte a indicar o encarregado pelo tratamento de dados pessoais. Essa desobrigação não pode acontecer porque a obrigação foi criada por uma norma legal. Uma resolução da ANPD não tem o condão de eximir qualquer pessoa física ou jurídica de uma obrigação prevista em lei. Poderia, de forma criativa, pensar em soluções que se coadunam com a situação concreta, a fim de não exigir obrigação de forma a exceder a capacidade da pessoa.

Nesse sentido, aos agentes de tratamento de que trata a minuta da resolução poderia se garantir formas alternativas de cumprimento da obrigação legal. Como, por exemplo, que se unam em grupos e tenham um único encarregado ou que seus quadros executivos acumulem tal função. Mesmo porque, além de ilegal, essa previsão colocaria tais agentes à margem dos negócios praticados na contemporaneidade porquanto, cada vez mais, serão relevantes as exigências acerca da proteção de dados pessoais, tanto entre o próprio mercado, quanto perante os titulares de dados.

Artigo 13 parágrafo único

> **Parágrafo único. O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação para que o titular de dados exerça os seus direitos previstos no art. 18 da LGPD, que será responsável pelo controle dos requerimentos dos titulares de dados, este departamento deve ser diverso do qual já implementado para utilização de outras práticas, como por exemplo o SAC.**

Artigo 14 caput e parágrafo único

> Art. 14. Os agentes de tratamento de pequeno porte devem adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados, **os serviços tecnológicos conexos oferecidos ou acessíveis através de sistemas e redes, as operações de tratamento que possuam alto risco aos direitos e liberdades das pessoas, a transigência quanto à frequência da admissão e desligamentos dos corpos administrativos** e a realidade **financeira do agente de tratamento que deve ter um investimento proporcional aos valores auferidos e declarados no último exercício à receita Federal do Brasil.**
>
> **Parágrafo único. A ANPD disponibilizará guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte até 60 (sessenta) dias após a publicação desta Lei, inclusive com medidas mais rigorosas para os agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares.**

Artigo 15 caput e parágrafo 3º

> Art. 15. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, **com o objetivo de protegê-los de acessos não**

autorizados a redes de comunicação eletrônica ou não, distribuição de códigos maliciosos e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito **com o objetivo de por fim á possíveis ataques e danos, visando a prevenção desses eventos.**

§3º Os **agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares de dados devem proporcionar e assegurar a segurança da rede e das informações com um dado nível de segurança a eventos acidentais ou ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos com boas práticas internas, além disso, deve promover aos seus subordinados treinamentos adequados sobre a proteção de dados pessoais, aprimoramento dos cuidados no exercício de sua função de acordo com a responsabilidade que desempenha no tratamento de dados pessoais, promover garantias, medidas e procedimentos internos de segurança da informação para atenuar riscos previstos no art. 46 da LGPD. Neste caso, os agentes de tratamento de pequeno porte deverão ter relatório interno de segurança da informação atualizado com parecer jurídico e técnico de sua eficácia e aplicabilidade.**