RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO

CONSTRUÇÃO DO MODELO REGULATÓRIO PARA APLICAÇÃO DA LGPD A MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE, *STARTUPS* E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS

AGOSTO/2021

RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO

CONSTRUÇÃO DO MODELO REGULATÓRIO PREVISTO PARA APLICAÇÃO DA LGPD A MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE, *STARTUPS* E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS

ELABORADO POR:

ISABELA MAIOLINO – CGN/ANPD

RODRIGO SANTANA DOS SANTOS – CGN/ANPD

Nota:

Esse Relatório de Análise de Impacto Regulatório é um instrumento de análise técnica, cujas informações e conclusões são fundamentadas nas análises promovidas pela equipe técnica da ANPD responsável pelo tema. Assim, não reflete necessariamente a posição final e oficial da ANPD, que somente se firma pela decisão de seu Conselho Diretor.

SUMÁRIO

1. INTRODUÇÃO[1]

A Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) aprovada para o ciclo 2021-2022 por meio da Portaria nº 11, de 27 de janeiro de 2021, incluiu dentre os seus temas prioritários o projeto regulatório relacionado à proteção de dados e da privacidade para pequenas e microempresas, *startup*s e pessoas físicas que tratam dados pessoais com fins econômicos.

A Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), prevê uma especial atenção às microempresas e empresas de pequeno porte, estabelecendo como competência da ANPD a edição de normativo sobre o assunto, conforme prevê o art. 55-J, inciso XVIII, *in verbis*:

> *Art. 55-J. Compete à ANPD:*
> *(...)*
> *XVIII - 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;*

O presente Relatório de Análise de Impacto Regulatório (AIR) avaliará os possíveis modelos regulatórios que podem ser constituídos para endereçar a previsão do art. 55-J, inciso XVIII, considerando, dentre outros aspectos, a garantia aos direitos dos titulares e aspectos como a natureza e o porte da entidade, o tipo do dado e o volume das operações de tratamento, bem como o estímulo à inovação, à digitalização e ao desenvolvimento econômico.

2. TOMADA DE SUBSÍDIOS

No dia 29 de janeiro de 2021, a ANPD publicou a Tomada de Subsídios nº 1/2021, nos termos da Nota Técnica nº 1/2021/CGN/ANPD (SEI nº 2361168), e estabeleceu um prazo de 30 dias para envio de contribuições. Para tanto, a ANPD disponibilizou em seu sítio eletrônico um formulário com os seguintes questionamentos:

(i) Quais são os desafios/problemas regulatórios relacionados ao tema?

(ii) Existem sugestões para endereçamento do problema?

(iii) Quais são as oportunidades relacionadas ao tema?

[1] O presente relatório de Análise de Impacto Regulatório contou com as contribuições de Adriana Macedo Marques, ex-servidora da ANPD.

(iv) Quais são as experiências internacionais sobre o tema?

(v) Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?

(vi) Como a União Europeia tem atuado para que agentes de tratamento de dados de pequeno porte estejam em conformidade com a *General Data Protection Regulation* (GDPR)?

(vii) Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?

(viii) Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?

(ix) Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?

(x) Quais são os impactos da implementação do tratamento de dados, inclusive sensíveis e de crianças e de adolescentes, em conformidade com a LGPD aos agentes de pequeno porte?

(xi) Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?

(xii) Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?

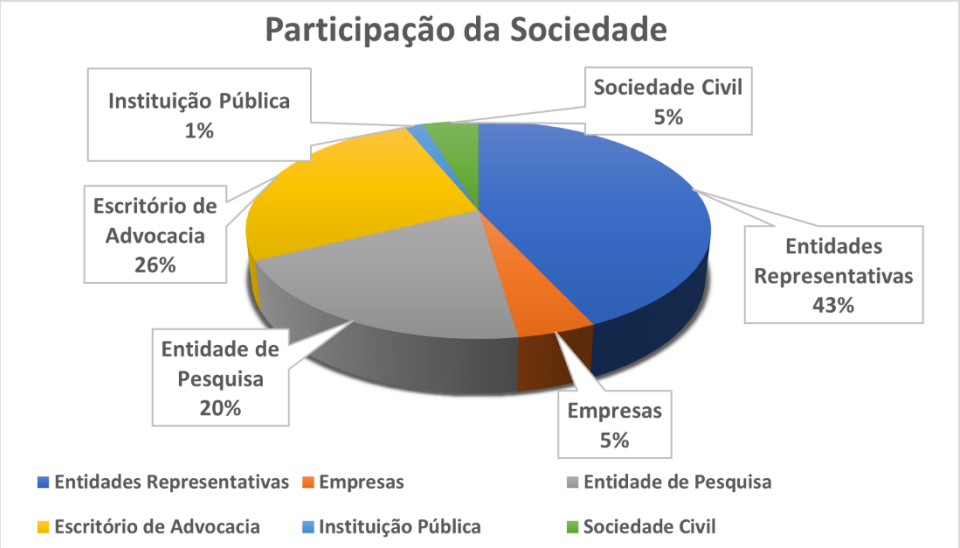
(xiii) Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?

(xiv) Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?

(xv) Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?

Foram recebidas 65 contribuições no prazo estipulado, contando com a participação de órgãos governamentais, entidades da sociedade civil, organismos de pesquisa, escritório de advocacia, associações e agentes de tratamento, como apresentado na figura a seguir:

Figura 1 – Resumo da participação na Tomada de Subsídios nº 1/2021



Fonte: Elaborado pela Coordenação-Geral de Normatização/ANPD

Além disso, ao longo da instrução processual e estudo do tema, a Coordenação-Geral de Normatização realizou reuniões com a empresa SpotMetrics (SEI nº 2406977); com a Lima & Feigelson Advogados (SEI nº 2408404); com a Data Privacy Brasil (SEI nº 2408845); com a Tudo sobre IoT (SEI nº 2408850); com representantes do Ministério da Economia, da Confederação Nacional da Indústria (CNI) e da Confederação Nacional de Jovens Empresários (CONAJE) (SEI nº 2559642); e com a Encarregada de dados do Ministério da Justiça de Portugal, a senhora Inês Oliveira (SEI nº 2483124).

3. ANÁLISE DE IMPACTO REGULATÓRIO

A flexibilização da aplicação da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais acaba por envolver várias obrigações estabelecidas pela referida lei. Além disso, a LGPD não conceitua o que seria microempresa e pequena empresa para fins da legislação.

Diante disso, optou-se por dividir a presente análise em 3 (três) grandes temas: (i) definição de microempresa, empresa de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais para fins de aplicação da norma; (ii) conformidade em relação às obrigações da LGPD; e (iii) segurança da informação.

Tendo em vista a complexidade do tema, foi inserido um último tópico apresentando uma síntese das conclusões e alternativas sugeridas ao longo deste relatório de AIR.

3.1 TEMA 1 - DEFINIÇÃO DE MICROEMPRESA, EMPRESA DE PEQUENO PORTE E *STARTUP*

3.1.1 RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

3.1.1.1 Introdução

Conforme já mencionado, ao dispor sobre as competências da ANPD, o art. 55-J, XVIII da LGPD previu que compete à ANPD editar normas específicas, com procedimentos simplificados e diferenciados 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 à LGPD.

Adicionalmente, convém citar a previsão de tratamento diferenciado prevista no Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, aprovado pela Lei Complementar nº 123, de 14 de dezembro de 2006 (Lei Complementar nº 123/2006), que, no art. 1º, §3º, garante que toda nova obrigação que atingir as microempresas e empresas de pequeno porte deve especificar, no instrumento que a instituiu, o tratamento diferenciado, simplificado e favorecido para o cumprimento.

Além disso, a Lei Complementar nº 182, de 1º de junho de 2021, que instituiu o marco legal das *startups* (Lei Complementar nº 182/2021), também prevê um tratamento diferenciado para essas entidades.

No entanto, não há, hoje, definição do que é esse grupo de empresas para fins de aplicação da LGPD, como será visto a seguir.

3.1.1.2 Quais os problemas a serem solucionados?

Muito embora a LGPD determine a edição de normas diferenciadas para esse grupo, não consta entre os conceitos do art. 5º da referida lei a definição de microempresa ou de empresa de

pequeno porte. Consequentemente, a regulamentação editada deve esclarecer quais critérios serão considerados pela ANPD ao editar normas, orientações e procedimentos simplificados e diferenciados, no intuito de atender o poder/dever do art. 55-J, XVIII da LGPD.

A identificação de critérios adequados é importante para que as normas e procedimentos simplificados incidam corretamente ao grupo ao qual se destina, considerando, entre outros aspectos, a garantia aos direitos dos titulares, o impacto financeiro que as obrigações da LGPD podem gerar nos agentes de tratamento de dados e o estímulo à inovação, à digitalização e ao desenvolvimento econômico.

Dentre as definições já estabelecidas pelo ordenamento brasileiro, vale citar que a Lei Complementar nº 123/2006 conceituou essas empresas em função de sua receita bruta anual, sendo esse um critério feito sob medida para atender o objeto e as disposições da referida lei:

> Art. 3º **Para os efeitos desta Lei Complementar, consideram-se microempresas ou empresas de pequeno porte**, a sociedade empresária, a sociedade simples, a empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei no 10.406, de 10 de janeiro de 2002 (Código Civil), devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que:
> I - no caso da microempresa, aufira, em cada ano-calendário, ***receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais)***; e
> II - no caso de empresa de pequeno porte, aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais). (Redação dada pela Lei Complementar nº 155, de 2016) [Grifamos]

No que se refere às iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, a Lei Complementar nº 123/2006 assim dispôs:

> Art. 65-A. (...).
> § 1º **Para os fins desta Lei Complementar, considera-se startup a empresa** de caráter inovador que visa a aperfeiçoar sistemas, métodos ou modelos de negócio, de produção, de serviços ou de produtos, os quais, quando já existentes, caracterizam startups de natureza incremental, ou, quando relacionados à criação de algo totalmente novo, caracterizam startups de natureza disruptiva.
> § 2º **As startups caracterizam-se por** desenvolver suas inovações em condições de incerteza que requerem experimentos e validações constantes, inclusive mediante comercialização experimental provisória, antes de procederem à comercialização plena e à obtenção de receita.
> (...)
> § 4º Os titulares de empresa submetida ao regime do Inova Simples preencherão cadastro básico com as seguintes informações:
> (...)

> II - descrição do escopo da intenção empresarial inovadora e definição da razão social, que deverá conter obrigatoriamente a expressão “Inova Simples (I.S.)”; [Grifamos]

A Lei Complementar nº 182/2021 também enquadra as startups com base em seu faturamento, dentre outros critérios, conforme o seu art. 4º:

> Art. 4º São enquadradas como startups as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.
> § 1º Para fins de aplicação desta Lei Complementar, são elegíveis para o enquadramento na modalidade de tratamento especial destinada ao fomento de startup o empresário individual, a empresa individual de responsabilidade limitada, as sociedades empresárias, as sociedades cooperativas e as sociedades simples:
> **I - com receita bruta de até R$ 16.000.000,00 (dezesseis milhões de reais) no ano-calendário anterior ou de R$ 1.333.334,00 (um milhão, trezentos e trinta e três mil trezentos e trinta e quatro reais)** multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 (doze) meses, independentemente da forma societária adotada;
> (...) [Grifamos]

A título de exemplo, convém citar que diversos outros entes e órgãos da administração pública federal adotaram variados critérios para segmentar a aplicação de suas respectivas legislações.

A Agência Nacional de Vigilância Sanitária (Anvisa)[2], para efeitos de aplicação de taxas de fiscalização de vigilância sanitária, considerou seis categorias de porte de empresa (Grupos I a IV, empresa de pequeno porte e microempresa) com base no seu faturamento anual.

A Agência Nacional de Telecomunicações (Anatel)[3], para fins de aplicação de variadas obrigações regulatórias (relacionadas por exemplo ao direito do consumidor, à competição, à certificação e à outorga) estipulou três categorias de porte de prestadora de serviço de

[2] BRASIL. Lei nº 9.872/1999. Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária, e dá outras providências.
ANVISA. Porte de Empresa. Disponível em: https://www.gov.br/anvisa/pt-br/acessoainformacao/perguntasfrequentes/administrativo/porte-de-empresa. Acesso em: 22 abr. 2021.
[3] ANATEL. Resolução nº 600/2012. Aprova o Plano Geral de Metas de Competição (PGMC). Brasília, Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2012/425-resolucao-600.
ANATEL. Resolução nº 632/2014. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (RGC). Brasília, Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2014/750-resolucao-632. Acesso em: 22 abr. 2021.

telecomunicações (prestadora de grande porte, prestadora de pequeno porte e prestadoras com menos de 5.000 acessos), com base na participação de mercado nacional.

A Agência Nacional de Aviação Civil (Anac)[4], para fins de aplicação de diversas obrigações regulatórias (como a guarda de registros, as medidas de segurança, as comunicações à Anac) estipulou as categorias de empresas com base na participação no mercado relevante; de aeronaves com base na capacidade de carga (passageiros ou tonelagem) e de aeródromos com base nos tipos de voo (regulares e não-regulares) e de serviço (aviação comercial e aviação geral).

O Instituto Brasileiro de Geografia e Estatística (IBGE)[5], para fins de classificação das empresas, fixou categorias de empresas com base no seu número de empregados.

O Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE)[6], apesar de também usar o número de empregados, fixou parâmetros bem distintos. O porte do estabelecimento é definido em função do número de pessoas ocupadas e depende do setor de atividade econômica, sendo classificado em indústria ou comércio e serviços.

O Banco Nacional de Desenvolvimento (BNDES)[7], por sua vez, classifica as empresas em porte com base na receita operacional bruta anual.

---

[4] ANAC. Resolução nº 342/2014. Regulamenta os documentos e as demonstrações contábeis padronizadas a serem apresentados pelas empresas brasileiras que exploram os serviços aéreos públicos, assim como aspectos de sua escrituração contábil, e dá outras providências. Brasília, Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/resolucoes-2014/resolucao-no-342-de-09-09-2014/@@display-file/arquivo_norma/RA2014-0342%20-%20Compilado%20at%C3%A9%20RA2017-0454.pdf.
ANAC. RBAC nº 153. Aeródromos – Operação, manutenção e resposta à emergência. Brasília, Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-153/@@display-file/arquivo_norma/RBAC153EMD06.pdf. Acesso em: 22 abr. 2021.

[5] IBGE. As Micro e pequenas empresas comerciais e de serviços no Brasil: 2001. Rio de Janeiro: IBGE, 2003, p 21. https://www.ibge.gov.br/estatisticas/economicas/outras-estatisticas-economicas/9123-as-micro-e-pequenas-empresas-comerciais-e-de-servicos-no-brasil.html?=&t=notas-tecnicas ou https://biblioteca.ibge.gov.br/visualizacao/livros/liv1898.pdf

[6] SEBRAE. Anuário do trabalho nos pequenos negócios: 2016. 9ed; DIEESE. São Paulo: DIEESE, 2018. https://www.sebrae.com.br/sites/PortalSebrae/estudos_pesquisas/empregodestaque13,46c9f925817b3410VgnVCM2000003c74010aRCRD ou https://www.sebrae.com.br/Sebrae/Portal Sebrae/Anexos/Anuário do Trabalho nos Pequenos Negócios 2016 VF.pdf

[7] BNDES. Guia do Financiamento. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/financiamento/guia/porte-de-empresa. Acesso em: 22 abr. 2021.

Diante dos exemplos acima, é possível observar que os critérios costumam ser definidos segundo características que façam sentido tanto em função das obrigações que se pretende regular quanto em função da atividade econômica relevante que as empresas desempenham.

Desse modo, além do porte econômico da empresa, a partir dos subsídios coletados por ocasião da Tomada de Subsídios nº 1/2021,[8] foram identificados outros critérios que devem ter sua adequação examinada pela ANPD para emprego na regulamentação, como, por exemplo: características da empresa (número de empregados, idade da empresa, natureza jurídica, ramo de atividade econômica), características dos dados tratados pelas empresas (dados comprados ou coletados, dados sensíveis, dados de criança e adolescente, dados sigilosos, dados de geolocalização, local de guarda); características do tratamento (finalidade, atividade regular ou esporádica, volume de dados, local de tratamento, tratamento sistemático, tratamento automatizado); e risco para o titular de dados (impacto sobre direitos e garantias fundamentais e sobre a privacidade), entre outros.

Portanto, decidir se determinada empresa, para fins de aplicação da LGPD, deve ter acesso a procedimentos simplificados e diferenciados não é uma tarefa tão simples quanto poderia parecer. Adicionalmente, a diversidade e quantidade de critérios sinalizam, de maneira inequívoca, que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados com fins econômicos constituem um universo heterogêneo de empresas sob os mais diversos aspectos.

Tal heterogeneidade é compatível com o que se observa no panorama nacional das empresas. Segundo dados do SEBRAE[9], as micro e pequenas empresas correspondem a 99% do total de empresas no Brasil, representam 29,5% do PIB nacional, são responsáveis por 55% dos empregos com carteira assinada e atuam em diferentes setores da economia (agropecuária, comércio, construção civil, indústria e serviços).

[8] Processo Sei nº 00261.000054/2021-37.

[9] SEBRAE. Sebrae e Frente Parlamentar pactuam com Bolsonaro medidas para garantir a sobrevivência das MPE. Brasília, Agência Sebrae de Notícias. Disponível em: http://www.agenciasebrae.com.br/sites/asn/uf/NA/sebrae-e-frente-parlamentar-pactuam-com-bolsonaro-medidas-para-garantir-a-sobrevivencia-das-mpe,c642c63524dc8710VgnVCM100000d701210aRCRD. Acesso em: 23 abr. 2021

3.1.1.3 A Autoridade tem competência para atuar sobre os problemas?

Nos termos do que dispõe o art. 55-J, XVIII da LGPD, a ANPD tem competência para editar normas específicas, com procedimentos simplificados e diferenciados, bem como os critérios de elegibilidade, 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 à LGPD.

3.1.1.4 Existe experiência internacional?

A definição de microempresas e empresas de pequeno porte se dá, em grande parte, em função do contexto doméstico, da legislação aplicável, do cenário econômico e dos direitos dos titulares. Todavia, é sempre oportuno observar como a questão foi abordada em outros países para compreender qual foi o tratamento do tema em outras jurisdições.

O tratamento conferido pela legislação da União Europeia ao disciplinar a proteção de dados pessoais e sua aplicação às microempresas e empresas de pequeno porte pode contribuir para o debate em direção a uma solução no Brasil, considerando a proximidade entre a LGPD e o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia[10].

O RGPD, assim como a LGPD, não traz o conceito de microempresa e empresa de pequeno porte. No entanto, essa definição já existia e constava na Recomendação 2003/361/EC[11], cujo artigo 2º do anexo traçou os contornos para microempresas, empresas de pequeno porte e médias empresas. A categoria de microempresas e empresas de pequeno porte é constituída por empresas que tenham menos de 50 funcionários e receita anual não superior a €$ 10 milhões.

Da mesma forma que a LGPD, o RGPD não isenta as microempresas e empresas de pequeno porte de cumprir as obrigações, mas prevê que suas peculiaridades sejam levadas em consideração (artigos 40.1 e 42.1, códigos de conduta e certificação).

[10] 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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504. Acesso em: 23 abr. 2021.

[11] Commission Recommendation 2003/361/EC. Concerning the definition of micro, small and medium-sized enterprises. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF. Acesso em: 23 abr. 2021.

A Austrália, por sua vez, dispôs que o *Privacy Act*[12] se aplica a todos os órgãos e entes governamentais e a todas as empresas com receita anual superior a Au$ 3 milhões. Ainda assim, previu hipóteses em que o *Privacy Act* se aplicaria a pequenas empresas (com receita anual inferior a Au$ 3 milhões), como, por exemplo, aquelas do setor privado de saúde, as que comercializem dados pessoais, que façam perfil de crédito, que tenham contrato com o governo ou com empresas abrangidas pelo *Privacy Act*, entre outras hipóteses.

A Califórnia, estado dos Estados Unidos da América, definiu em seu *Consumer Privacy Act* de 2018 que para fins daquela legislação, 50% do faturamento dos negócios das empresas deve advir da venda de dados pessoais de consumidores, bem como devem tratar com fins comerciais os dados pessoas de 50.000 ou mais consumidores. Caso contrário, a referida legislação não se aplica.

3.1.1.5 Quais os objetivos da ação? Por que a intervenção regulatória é necessária?

O objetivo imediato da intervenção regulatória é atender ao comando do art. 55-J, XVIII da LGPD e editar norma específica, simplificando e diferenciando os procedimentos para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam se adequar à LGPD.

Constituem contornos dessa norma específica o compromisso de garantir os direitos dos titulares de dados, o equilíbrio entre as regras constantes da LGPD e o porte do agente de tratamento de dados, buscando incentivar a inovação e o desenvolvimento econômico.

O objetivo mediato é facilitar a adaptação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais à LGPD, promovendo a sua conformidade com a lei e contribuindo para a disseminação da cultura de proteção de dados pessoais.

Especificamente no que se refere ao tema relacionado à definição desse grupo de agentes de tratamento, pretende-se apresentar uma proposta de conceito que permita à ANPD estabelecer contornos claros para aplicação da legislação de proteção de dados pessoais compreensível a essas empresas.

[12] OAIC. Rights and Responsibilities. Disponível em: https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/#who-has-responsibilities-under-the-privacy-act. Acesso em: 23 abr. 2021.

3.1.1.6 Quais os grupos afetados?

A norma de aplicação da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais impacta todos os titulares de dados que se relacionam com esses agentes de tratamento. Diante disso, ao proceder o levantamento dos agentes econômicos, dos usuários dos serviços prestados e dos demais afetados pelo problema ora analisado, os grupos a seguir foram identificados como mais impactados:

i) agentes de tratamento de dados, em especial aqueles em que se enquadram as microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais;

ii) titulares de dados pessoais;

iii) fabricantes de *softwares* de gestão e governança de dados;

iv) prestadores de serviço de consultoria;

v) encarregados.

Outros grupos identificados, como órgãos de pesquisa, órgãos públicos, agências reguladoras e imprensa poderão ser afetados, mas com impactos reduzidos ou na medida em que se relacionarem com microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

3.1.2 ANÁLISE DAS ALTERNATIVAS

3.1.2.1 Quais são as opções regulatórias consideradas para o tema?

A partir do exposto, para solução do problema de definição do conceito de microempresa, empresa de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais a fim de determinar o acesso a procedimentos simplificados e diferenciados, consideram-se alternativas possíveis tanto (i) uma abordagem baseada numa definição única e geral quanto (ii) uma abordagem baseada numa definição circunstancial, em que os critérios variam à luz de cada obrigação e dos riscos associados.

Diante da diversidade dos critérios que devem ser considerados na regulamentação da aplicação da LGPD a esse grupo de agentes de tratamento, como características da empresa,

características dos dados pessoais, características do tratamento e risco para o titular de dados, e da heterogeneidade do universo de microempresas, empresas de pequeno porte e *startup*s, considerou-se mais importante privilegiar a flexibilidade do conceito de microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais à luz das obrigações da LGPD.

Além disso, entende-se importante o estabelecimento de um segundo critério relacionado ao tipo de tratamento realizado por esse grupo de empresas, a fim de que o titular de dados pessoais não seja prejudicado com a edição do normativo. Ademais, não seria racional estabelecer o mesmo parâmetro para todas as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, pois nem todo tratamento de dado pessoal para fins da norma a ser indicada implicaria, necessariamente, atenção especial pela ANPD.

Nesse sentido, algumas opções foram levantadas. A primeira delas diz respeito à diferenciação ao tipo de tratamento realizado pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, ou seja, se ele é realizado de forma regular e principal, que consistiria naquele realizado para um determinado percentual da receita bruta anual; ou de forma incidental, sendo este último aquele realizado para fins administrativos ou para contato com usuários de bens e serviços ofertados.

Essa opção implicaria uma definição circunstancial de microempresa, empresa de pequeno porte, *startups* e pessoa física que trata dado pessoal para cada obrigação elencada na norma. Isso poderia tornar menos simples para esses agentes de tratamento a compreensão de suas obrigações. Por outro lado, essa abordagem permite maior grau de simplificação e facilitação do atingimento da conformidade dessas obrigações.

Outra opção regulatória consiste em simplificar o atendimento das obrigações da LGPD com base no risco que o tratamento de dados realizado apresenta aos titulares de dados pessoais, sendo então necessária a apresentação do que esta ANPD entende como risco para fins da norma.

A definição conceitual em relação ao que a ANPD compreende como destinatários da norma e como microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais foi amplamente debatida ao longo dos tópicos anteriores. No caso, independentemente de outros critérios que venham a ser adotados pela norma, entende-se que essa conceituação deve

ser feita e, conforme exposto, sugere-se que sejam adotados os conceitos já trazidos pela legislação, como a Lei Complementar nº 123/2006 e a Lei Complementar nº 182/2021.

No entanto, além da conceituação, é necessário avaliar as outras opções relacionadas à aplicação da norma.

3.1.2.2 Alternativa A – Aplicação da norma pelo faturamento e pelo volume de dados tratados

Para fins de aplicação da norma, é possível diferenciar o tipo de tratamento realizado pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, ou seja, se ele é realizado de forma regular e principal. No caso, o tratamento como atividade principal consiste naquele realizado para obtenção de 50% (cinquenta por cento) ou mais da receita bruta anual; e o de forma incidental consiste naquele realizado para fins administrativos ou para contato com usuários de bens e serviços ofertados. Essa classificação tem como inspiração a norma estabelecida pelo *California Consumer Privacy Act*, de 2018.

Muito embora esse critério pareça objetivo, é de difícil aferição, seja em razão da dificuldade de acesso à documentação contábil da empresa, seja em razão da dificuldade de se aferir (mesmo de posse dos documentos contábeis) o quanto, de fato, de sua receita advém da atividade de tratamento de dados pessoais. Muito embora os documentos contábeis sigam algum grau de padronização, há uma margem razoável para que as empresas eventualmente classifiquem as receitas de formas diferentes. Assim, essa regra poderá criar incentivos econômicos para que empresas classifiquem determinadas receitas para outras classificações contábeis, a fim de obter um tratamento diferenciado na legislação de proteção de dados.

Além disso, o potencial de risco e a probabilidade de danos graves para titulares de dados pessoais não possui relação direta com a receita bruta (ou, ainda, com o percentual de faturamento que decorre da atividade de tratamento de dados pessoais).

Resumo da análise da alternativa A

Grupos afetados	Desafios	Benefícios
ANPD	Dificuldade em auferir o faturamento das empresas	Critério específico para aplicação da norma
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Dificuldade em comprovar que o faturamento advém do tratamento de dados pessoais	Fácil identificação do tratamento incidental de dados pessoais

Titulares de dados pessoais	Atividades de alto risco para os titulares podem ser incluídas na flexibilização, diminuindo a proteção dos seus direitos	Não foram identificados benefícios relevantes.
Fabricantes de *softwares* de gestão e governança de dados	Não foram identificados desafios relevantes.	Não foram identificados benefícios relevantes.
Prestadores de serviço de consultoria	Não foram identificados desafios relevantes.	Não foram identificados benefícios relevantes.
Encarregados	Não foram identificados desafios relevantes.	Não foram identificados benefícios relevantes.

3.1.2.3 Alternativa B – Aplicação da norma em razão do risco

A adoção de critérios de flexibilização da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais com base no risco que o tratamento realizado apresenta aos titulares de dados pessoais é uma opção que foi aventada em algumas contribuições recebidas ao longo da Tomada de Subsídios nº 1/2021. No caso, ela implicaria em desconsiderar o faturamento auferido com o tratamento de dados ou o tipo de tratamento realizado (ou seja, incidental ou principal), aventando somente o risco que esse tratamento pode causar aos titulares de dados pessoais.

Com isso, seria necessário estabelecer, ainda que de forma inicial, o que a ANPD entende como tratamento de alto risco para os titulares de dados pessoais. Tendo em vista ser um conceito para o qual não há definição homogênea na experiência internacional e que também é utilizado para outros temas relacionados à proteção de dados pessoais, como elaboração de relatório de impacto à proteção de dados pessoais e incidentes de segurança, para que essa opção seja adotada é necessário estabelecer critérios que façam sentido especificamente ao que a norma se propõe. Outra opção é que a norma deixe claro que a ANPD poderá estabelecer o critério a partir de casos concretos.

Além disso, seria preciso trazer a ideia de larga escala do tratamento de dados pessoais, tendo em vista que o mero tratamento de dados pessoais sensíveis, por exemplo, não necessariamente traz um alto risco aos titulares. Assim, o tratamento de larga escala seria aquele que abrange um número significativo de titulares, considerando também o volume de dados envolvidos, a duração, a frequência e a extensão geográfica do tratamento realizado.

Tendo em vista que a norma não definirá de forma exata o que seria número significativo de titulares em razão de ser a primeira norma dessa natureza e não se ter parâmetros na LGPD ou em outras legislações tanto brasileiras quanto estrangeiras, é possível que, em um primeiro momento, esse ponto gere insegurança jurídica às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Resumo da análise da alternativa B

Grupos afetados	Desafios	Benefícios
ANPD	Necessidade de maior estudo e maturidade na definição de tratamento de alto risco para o titular de dados.	Maior harmonia com os conceitos utilizados internacionalmente. Maior facilidade de enquadramento para aplicação da norma para fins de fiscalização da ANPD.
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Insegurança em relação ao conceito de risco. Insegurança em relação à não definição do que vem a ser alto volume ou número significativo de titulares para ANPD.	A aplicação da norma se torna mais ampla e tende a atingir um número maior desses agentes. Oportunidade de negócios em outros países, considerando que o conceito de risco para os titulares é bastante utilizado internacionalmente.
Titulares de dados pessoais	Percepção de demora na efetividade da regulamentação, tendo em vista necessidade de maior estudo e maturidade para a definição mais objetiva de tratamento de alto risco.	As atividades de tratamento que geram maior risco não são atingidas pela flexibilização, preservando os direitos dos titulares de dados pessoais.
Fabricantes de *softwares* de gestão e governança de dados	Custo de adaptação ao novo modelo regulatório.	O conceito de risco é bastante utilizado nos *softwares* de gestão e governança de dados.
Prestadores de serviço de consultoria	Necessidade de adaptação ao novo modelo e conhecimento maior da regulamentação e das demais manifestações da ANPD.	O conceito de risco é bastante difundido no tema de proteção de dados.
Encarregados	Necessidade de conhecimento com relação ao conceito de risco.	Não foram identificados benefícios relevantes.

3.1.3 CONCLUSÃO E ALTERNATIVA SUGERIDA

3.1.3.1 Qual a conclusão da análise realizada?

Considerando as alternativas apresentadas como solução para os problemas relacionados à definição de microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam

dados pessoais, identificou-se que, em razão dos desafios e benefícios elencados para cada um dos grupos afetados, que a **Alternativa B** é a mais adequada para endereçar o tema.

Ao privilegiar a flexibilidade do conceito de microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, variando de acordo com as obrigações, aumenta-se a capacidade de a norma considerar os critérios adequados que permitam a simplificação e flexibilização de determinada obrigação sem aumentar consideravelmente os riscos envolvidos tanto para os titulares de dados quanto para esse grupo de agentes de tratamento.

Essa flexibilidade ocorre ao se combinar um conceito base de microempresas, empresas de pequeno porte e *startups*, com os demais critérios identificados ao longo do processo de coleta de informações, como as contribuições da Tomada de Subsídios nº 1/2021.

Nesse sentido, revelam-se como apropriados, até mesmo a título de uniformidade, adotar como conceitos-base os trazidos pela Lei Complementar nº 123/2006 para microempresas, empresas de pequeno porte e *startups*:

> Art. 3º **Para os efeitos desta Lei Complementar, consideram-se microempresas ou empresas de pequeno porte**, a sociedade empresária, a sociedade simples, a empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei no 10.406, de 10 de janeiro de 2002 (Código Civil), devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que:
> I - no caso da microempresa, aufira, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais); e
> II - no caso de empresa de pequeno porte, aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais). (Redação dada pela Lei Complementar nº 155, de 2016) [Grifamos]
>
> Art. 65-A. (...).
> § 1º **Para os fins desta Lei Complementar, considera-se startup a empresa** de caráter inovador que visa a aperfeiçoar sistemas, métodos ou modelos de negócio, de produção, de serviços ou de produtos, os quais, quando já existentes, caracterizam startups de natureza incremental, ou, quando relacionados à criação de algo totalmente novo, caracterizam startups de natureza disruptiva.
> § 2º **As startups caracterizam-se por** desenvolver suas inovações em condições de incerteza que requerem experimentos e validações constantes, inclusive mediante comercialização experimental provisória, antes de procederem à comercialização plena e à obtenção de receita.
> (...)
> § 4º Os titulares de empresa submetida ao regime do Inova Simples preencherão cadastro básico com as seguintes informações:
> (...)

> II - descrição do escopo da intenção empresarial inovadora e definição da razão social, que deverá conter obrigatoriamente a expressão “Inova Simples (I.S.)”; [Grifamos]

Além disso, para *startups*, cabe também adotar os parâmetros trazidos pela Lei Complementar nº 182/2021, conforme o seu art. 4º, para fins de faturamento máximo para os agentes econômicos aos quais a resolução se destina:

> Art. 4º São enquadradas como startups as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.
> § 1º Para fins de aplicação desta Lei Complementar, são elegíveis para o enquadramento na modalidade de tratamento especial destinada ao fomento de startup o empresário individual, a empresa individual de responsabilidade limitada, as sociedades empresárias, as sociedades cooperativas e as sociedades simples:
> I - com receita bruta de até R$ 16.000.000,00 (dezesseis milhões de reais) no ano-calendário anterior ou de R$ 1.333.334,00 (um milhão, trezentos e trinta e três mil trezentos e trinta e quatro reais) multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 (doze) meses, independentemente da forma societária adotada;
> (...)

Esses conceitos serão considerados em conjunto com outros critérios especificados ao longo do regulamento, tendo em vista que entidades que não se enquadram nos conceitos acima mas que, ao se pensar na lógica do que se pretende com essa norma de aplicação da LGPD, podem ser equiparadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, quais sejam, as pessoas jurídicas sem fins lucrativos, como associações, fundações, organizações religiosas, partidos políticos e demais entidades equiparadas, incluídas as pessoas formais.

Em relação às pessoas físicas que tratam dados pessoais, sugere-se que essa categoria se refira às pessoas naturais que tratam dados pessoais, guardando assim relação com os termos da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil).

Entende-se que esse grupo de agentes de tratamento deve ter uma denominação específica a ser apresentada na norma a ser editada, sugerindo-se, aqui, a adoção do termo agentes de tratamento de pequeno porte. Esse termo denota a principal categoria que compõe o grupo de entidades às quais se destina a norma a ser editada e que a LGPD determina que sejam editadas normas com um regime diferenciado, qual seja, às microempresas e às empresas de pequeno porte.

Além disso, o termo também guarda referência com a Lei Complementar nº 123/2006, sem perder a conexão direta com os termos estabelecidos pela LGPD, em especial com os agentes de tratamento de dados pessoais.

Em relação ao segundo critério da norma, optou-se por adotar a classificação do tratamento realizado em razão do risco que ele implica aos titulares de dados, tendo em vista ser mais efetivo na proteção dos direitos dos titulares de dados, ao tempo em que gera menos insegurança para fins do trabalho de fiscalização da ANPD.

Assim, sugere-se que os mesmos conceitos e critérios relacionados ao conceito desse grupo de agentes de tratamento e ao risco relacionado à atividade de tratamento se aplicam a todas as obrigações elencadas na norma.

3.1.3.2 Como será operacionalizada a alternativa sugerida?

Para operacionalização da alternativa escolhida, serão estabelecidos como critérios-base de identificação e definição dos agentes de tratamento de pequeno porte os seguintes conceitos: (i) microempresas, empresas de pequeno porte e *startups* como aqueles indicados na Lei Complementar nº 123/2006; e (ii) demais entidades, como pessoas jurídicas sem fins lucrativos. Além disso, esse conjunto de entes deve ter como faturamento máximo os valores estabelecidos pela Lei Complementar nº 182/2021.

Para fins de classificação quanto ao tipo de tratamento realizado, optou-se por adotar o critério relacionado ao risco que o tratamento de dados pessoais acarreta ao titular de dados, tendo em vista ser um modelo de mais fácil operacionalização pela área de fiscalização da ANPD. Além disso, entende-se que esse critério resguarda de forma mais efetiva os titulares de dados pessoais, sem impedir que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais se beneficiem de um tratamento diferenciado, em especial aqueles que realizam apenas o tratamento de dados de funcionários ou relacionados à sua gestão administrativa.

<u>Tratamento de alto risco</u>

Para fazer uso de critérios relacionados ao risco referente ao tratamento de dados, seria indicado que a ANPD apresentasse o conceito a ser adotado para fins da norma. Há que se considerar, no entanto, a dificuldade de se definir risco para fins da flexibilização da aplicação da

LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoas e a necessidade de se estabelecer critérios mínimos para análise.

Sobre a definição de tratamento de alto risco para titulares de dados, ressalta-se que a avaliação do risco é bastante utilizada pelas autoridades de proteção de dados. A título de exemplo, destacam-se os documentos emitidos pelas autoridades do Reino Unido (*Information Commissioner's Office* - ICO)[13] e da França (*Commission Nationale de Informatique et des Libertés* - CNIL)[14], que utilizam o conceito de avaliação do risco no tratamento dos dados dos titulares.

Ademais, vale ainda citar o *Guideline*[15] sobre relatório de impacto à proteção de dados pessoais da Comissão Europeia. Ainda que não seja endereçado exclusivamente a empresas de pequeno porte, o guia trata da definição de alto risco, utilizando critérios como tratamento de dados em larga escala e de dados sensíveis, dados de crianças e adolescentes e de idosos, e que foi considerado ao longo dos estudos sobre o tema pela área técnica da ANPD.

Diante disso, destaca-se a possibilidade de definição de um rol taxativo de atividades que poderiam acarretar alto risco, como o tratamento de dados sensíveis e de grupos vulneráveis (incluindo dados de crianças, de adolescentes e de idosos), o uso de tecnologias emergentes e o tratamento automatizado de dados pessoais.

Além disso, considerando que a mera identificação das hipóteses acima listadas não é suficiente para se estipular uma atividade de alto risco, é necessário também endereçar a questão relacionada à escala do tratamento de dados pessoais.

Larga escala

Definir o que é larga escala no que se refere ao tratamento de dados pessoais não é tarefa trivial, tendo em vista a inexistência, no atual momento, de parâmetros que permitam auferir o volume de dados de fato tratados por microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

[13] ICO. Data storage, sharing and security. Disponível em: https://ico.org.uk/for-organisations/sme-web-hub/frequently-asked-questions/data-storage-sharing-and-security/#howdo. Acesso em 02/08/2021.
[14] CNIL. Guide pratique de sensibilisation au RGPD. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf. Acesso em 02/08/2021.
[15] EC. Guidelines on Data Protection Impact Assessment (DPIA). Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 02/08/2021.

Assim, é necessário que a norma estabeleça critérios abertos relacionados a esse conceito que possam ser interpretados pela ANPD e atualizados ao longo do tempo, a fim de que a norma não institua parâmetros que não se baseiem em evidências concretas. Além disso, a norma deve prever orientações futuras da ANPD sobre o assunto, a fim de que se possa diminuir os custos relacionados à eventual insegurança jurídica em razão dos conceitos abertos adotados.

3.1.3.3 Como a alternativa sugerida será monitorada?

A norma proposta não estabelece indicadores objetivos sobre o tema. Entretanto, por meio do acompanhamento das atividades de fiscalização da Coordenação-Geral de Fiscalização, bem como por meio de elaboração dos relatórios anuais de gestão da ANPD, será possível aferir se as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais estão cumprindo a LGPD nos termos da resolução.

Nesse sentido, sugere-se acompanhar a quantidade de reclamações de titulares de dados em face às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, e a quantidade de processos sancionatórios instaurados contra eles. Uma vez que não existem dados históricos sobre essas informações, a coleta e o acompanhamento desses dados poderão servir de base para eventuais revisões da alternativa escolhida.

3.2 TEMA 2 – CONFORMIDADE DAS OBRIGAÇÕES DA LGPD PELAS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E *STARTUPS* E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS

3.2.1 RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

3.2.1.1 Introdução

Sobre a conformidade em relação às regras da LGPD, a lei impõe aos agentes de tratamento de dados pessoais, inclusive às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, diversas obrigações, como a necessidade de atender a solicitações do titular sem custos para este e nos prazos previstos em regulamento; manutenção do registro das operações de tratamento de dados pessoais; elaboração de relatório de impacto à proteção de dados pessoais; tratamento de dados em conformidade com a legislação; indicação do encarregado de tratamento de dados pessoais; portabilidade de dados dos titulares; e a garantia de segurança e ao sigilo de dados pessoais.

Por outro lado, conforme já mencionado, a LGPD dispõe no art. 55-J, XVIII que compete à ANPD editar normas específicas, com procedimentos simplificados e diferenciados para que microempresas, empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, possam adequar-se à LGPD

No tema 1 deste relatório foram analisados os critérios que devem ser considerados para a definição das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais como integrantes da categoria específica de agente de tratamento, cujo nome será definido em norma específica. Preliminarmente, observa-se que para essa flexibilização, além do critério de porte do agente de tratamento, entendeu-se ser necessário outra importante variável, que diz respeito ao tratamento de dados de alto risco.

Assim, neste tópico serão analisadas as possíveis obrigações que podem ser simplificadas para aqueles classificados nessa categoria de agentes.

Cabe ressaltar que um dos maiores desafios deste normativo refere-se ao fato de que se busca simplificar regras que ainda serão tratadas em regulamentação específica, como por exemplo, a comunicação de incidentes, o relatório de impacto à proteção de dados e a obrigatoriedade de indicação de encarregado de dados pessoais, temas já previstos na Agenda Regulatória 2021-2022 da ANPD e que, em sua maioria, já tiveram o processo de regulamentação iniciado[16].

Entretanto, tendo em vistas os custos e dificuldades de adaptação à LGPD enfrentados por esse grupo de agentes, entende-se oportuno endereçar a importância do estabelecimento de obrigações simplificadas, bem como analisar e sugerir as possíveis formas de endereçar o tema em uma norma.

3.2.1.2 Quais os problemas a serem solucionados

Ao longo da Tomada de Subsídios realizada, o principal problema identificado consiste na elevada carga regulatória ocasionada pelas obrigações dispostas na LGPD, que podem causar grave impacto na operação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. A título de exemplo, foi citado nas contribuições o levantamento

[16] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022.

disponibilizado pelo SEBRAE[17] de que existem aproximadamente 19.228.025 empresas, sendo que, destas, 9.810.483 são microempreendedores individuais (MEI) (51,02%) e 6.586.497 são microempresas (34,25%). Dessa forma, percebe-se que 85,27% das empresas do País são microempreendedores individuais e microempresas, de maneira que seu desempenho possui um alto impacto na economia do País, com geração de renda e emprego para milhares de famílias brasileiras.

Ademais, pode-se inferir que a receita dessas empresas não é alta, considerando que para assim serem classificadas, devem possuir faturamento anual igual ou inferior ao valor estimado de R$ 360.000,00, conforme disposto na Lei Complementar nº 123/2006.

Quanto às *startups*, segundo levantamento da Associação Brasileira de Startups (Abstartups), existem mais de 12.700 empresas assim classificadas como startups no País[18]. Segundo o Perfil da Startup Brasileira (Radiografia do Ecossistema Brasileiro de Startups)[19], 63% das startups contam com até 5 pessoas, 49% são compostas apenas pelos sócios, 69% têm faturamento abaixo de R$ 50.000,00 e 15% possuem faturamento anual entre R$ 50.000,00 e R$ 250.000,00, 69% têm até 3 anos de funcionamento e apenas 69,7% possuem o CNPJ formalizado junto aos órgãos oficiais. Ou seja, com o diminuto número de funcionários e com um faturamento limitado, novas obrigações, que poderiam demandar a contratação de corpo técnico especializado, podem causar diversas dificuldades ao funcionamento desse grupo de empresas.

Por outro lado, o porte de uma empresa não altera o direito que o titular de dados tem à proteção de seus dados pessoais, nos termos do art. 17 e seguintes da LGPD, nem desobriga que as atividades de tratamentos de dados pessoais observem a boa-fé e os princípios elencados no art. 6º do mesmo normativo, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

---

[17] Painel de empresas. Disponível em: https://datasebrae.com.br/totaldeempresas/. Dados de maio, 2020. Acesso em 24/07/2021.

[18] G1.Globo.com. Globonews. Número de startups no Brasil aumentou 20 vezes nos últimos oito anos. 11 já são unicórnios. Disponível em https://g1.globo.com/globonews/noticia/2020/01/15/numero-de-startups-no-brasil-aumentou-20-vezes-nos-ultimos-oito-anos-11-ja-sao-unicornios.ghtm. Acesso em 24/07/2021.

[19] O Momento da Startup Brasileira e o futuro do Ecossistema de Inovação. Disponível em: https://abstartups.com.br/radiografia-do-ecossistema/. Acesso em 24/07/2021.

Outro problema identificado é a baixa cultura de proteção de dados nas microempresas, nas empresas de pequeno porte, nas *startups* e das pessoas físicas que tratam dados pessoais. Esse problema pode ser ocasionado pela falta de conhecimento da LGPD, pela falta de apoio técnico especializado, pela falta de estrutura para absorver todas as diretrizes, princípios e regras dispostas na LGPD, bem como por outros fatores não listados.

Além disso, cabe destacar que a LGPD foi promulgada em 2018 e só entrou em vigor em sua totalidade em 2021, ou seja, é uma lei recente e pode não ser conhecida em sua totalidade por alguns grupos de agentes econômicos, e as suas disposições podem ser vistas como complexas para esse grupo de empresas.

Essa baixa cultura de proteção de dados identificada na mencionada categoria especial de agentes de tratamento pode levar a uma baixa compreensão dos riscos relacionados às violações de normas de proteção de dados pessoais e, eventualmente, pode gerar dano aos titulares dos dados pessoais. Esse fato pode elevar o número de reclamações contra esse grupo de agentes de tratamento por parte dos titulares de dados pessoais e, consequentemente, gerar eventual desconfiança no ecossistema de proteção de dados pessoais.

3.2.1.3 A Autoridade tem competência para atuar sobre os problemas?

Nos termos do que dispõe o art. 55-J, XVIII da LGPD, a ANPD tem competência para editar normas específicas, com procedimentos simplificados e diferenciados, bem como os critérios de elegibilidade, para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam adequar-se à LGPD.

3.2.1.4 Existe experiência internacional?

No que concerne a experiências internacionais relacionadas à conformidade de obrigações legais ou regulatórias por microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, cabe esclarecer que foram identificadas duas abordagens: i) instrumentos para promover a cultura de proteção de dados e ii) regulamentação para dispensa ou flexibilização de obrigações.

Quanto aos instrumentos para promover a cultura de proteção de dados em microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, existem diversas experiências internacionais. No entanto, o presente relatório de AIR apresentará os casos do Reino

Unido e da União Europeia, tendo em vista que essas experiências podem contribuir para o debate em direção a uma solução para o Brasil, considerando a proximidade entre a LGPD e o RGDP.

A ICO, autoridade de proteção de dados do Reino Unido, possui um sistema online que fornece apoio aos pequenos negócios. A título de exemplo, a ICO tem uma página web dedicada às pequenas e médias empresas, que esclarece as principais dúvidas das organizações, fornece o guia "*Getting it right: a brief guide to data protection for small businesses*"[20], apresenta orientações quanto às principais obrigações que devem ser seguidas por esse grupo de empresas, e apresenta um "*Accountability Framework*"[21], com objetivo de facilitar o entendimento das empresas com relação à conformidade com a RGPD.

Além disso, foi criado o *ICO Innovation Hub*[22] que, em conjunto com reguladores de outros setores, como por exemplo, financeiro e saúde, promove iniciativas relacionadas à proteção de dados implementadas por empresas inovadoras ou *startups*.

Já na União Europeia, diversos países têm iniciativas para fortalecer a cultura de privacidade e proteção de dados, entre os quais podemos destacar a iniciativa da autoridade francesa, a CNIL, que possui um guia orientativo do RGPD voltado a pequenas e médias empresas, o "*Guide pratique de sensibilisation au RGPD*"[23]. Por sua vez, o *Ireland Data Protection Commissioner* (Irish DPC), autoridade irlandesa, publicou um guia para pequenas e médias empresas[24], que contém um *checklist* para orientar os agentes na conformidade com o RGDP.

As experiências internacionais relacionadas às dispensas ou flexibilizações de obrigações legais e regulatórias serão apresentadas a seguir, sendo divididas pelas principais obrigações.

Obrigações relacionadas aos direitos do titular

[20] ICO. Getting it right: a brief guide to data protection for small businesses. Disponível em: https://ico.org.uk/media/for-organisations/documents/1559/getting_it_right_a_brief_guide_to_data_protection_for_smes.pdf. Acesso em 27/07/2021.
[21] ICO. Accountability Framework. Disponível em: https://ico.org.uk/for-organisations/accountability-framework/. Acesso em 27/07/2021.
[22] ICO Innovation Hub. Disponível em: https://ico.org.uk/about-the-ico/research-and-reports/ico-innovation-hub-project-report/. Acesso em 27/07/2021.
[23] CNIL. Guide pratique de sensibilisation au RGDP. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf. Acesso em 27/07/2021
[24] Irish DPC. GDPR Guidance for SMEs. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf. Acesso em 27/07/2021.

O RGPD não apresenta flexibilizações para pequenas empresas no que se refere às obrigações que a norma estabelece. No entanto, cabe apresentar o posicionamento da referida norma sobre as obrigações relacionadas aos direitos do titular, tendo em vista que uma das análises que serão feitas diz respeito à flexibilização dessa categoria de obrigações estabelecidas pela LGPD e que ainda não foram normatizadas pela ANPD.

No caso, o RGPD dispõe sobre o direito de acesso às informações pelos titulares de dados nos artigos 12 e 15.

No artigo 12, o RGPD informa que o controlador deve adotar as medidas adequadas para fornecer ao titular as informações a respeito do tratamento de dados pessoais, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. As informações podem ser prestadas por escrito ou por outros meios, incluindo meios eletrônicos. Se o titular dos dados solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios. O prazo para atendimento é de 30 dias, podendo ser prorrogado por mais 30 caso a requisição seja mais complexa. A resposta é feita pelo mesmo instrumento em que recebida, ou seja, se houve recebimento por e-mail, a resposta também será por e-mail, exceto se o requerente solicitar por outro meio.

Já no artigo 15, o RGPD prevê que o titular dos dados tem o direito de obter do controlador a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acesso aos seus dados pessoais e a outras informações suplementares. Para responder a essa solicitação, o controlador fornece uma cópia dos dados pessoais objeto de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrônicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrônico de uso corrente.

Registro das Atividades de Tratamento

O RGPD prevê o registro das atividades de tratamento de dados pessoais, descrevendo quais informações devem ser registradas, tanto pelo operador, quanto pelo controlador – ao contrário da LGPD, que não traz esses pormenores sobre que informações devem ser registradas, apenas dispondo que “o controlador e o operador devem manter registro das operações de tratamento de

dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (art. 37 da LGPD). Além disso, o RGPD diferencia as informações que devem ser registradas para o controlador (artigo 30) e para o operador (art. 31).

Especificamente no que se refere a pequenas empresas, o artigo 30 prevê uma exceção para o registro de atividade para empresas que possuam menos de 250 funcionários, as quais não precisam manter registros do procedimento de tratamento de dados da mesma forma que outras empresas. A obrigação apenas não é afastada em 3 casos: quando os tratamentos realizados tenham alto potencial de resultar em um risco para os direitos e liberdades dos titulares, quando eles forem tratamentos habituais ou, por fim, quando incluírem dados de categoria especial ou dados relacionados a ofensas e condenações criminais.

Relatório de Impacto à Proteção de Dados Pessoais

O artigo 35 do RGPD prevê a obrigação de elaborar uma avaliação de impacto à proteção de dados pessoais por todas as organizações que executam atividades de risco elevado. De acordo com esse artigo, o *Data Protection Impact Assessment* (DPIA) é necessário quando algum tratamento, principalmente que implique na utilização de novas tecnologias, seja suscetível de resultar em alto risco para os direitos e liberdades dos titulares, considerando a sua natureza, escopo, contexto e finalidade.

Nesse caso, não há exceções para microempresas e empresas de pequeno porte quando as atividades desempenhadas pela organização implicam alto risco à proteção de dados pessoais.

No mesmo sentido, o "*Guidelines on Data Protection Impact Assessment* (DPIA)", elaborado pelo *Article 29 Working Party* e ratificado pelo *European Data Protection Board*, complementou o rol de situações que poderiam resultar em alto risco, trazendo outras 9 operações ao rol não exaustivo já trazido pelo artigo 35 do RGPD.

Observa-se que tanto o RGPD, quanto as orientações do *Article 29 Working Party*, não levam em consideração a natureza jurídica do agente de tratamento para definir a necessidade ou não de apresentação do DPIA.

Comunicação de Incidentes de Segurança

Cabe esclarecer que não foi encontrada na pesquisa experiência internacional um instrumento normativo endereçado exclusivamente às microempresas e empresas de pequeno porte que os desobrigue do envio da comunicação de incidente.

Ainda que não tenham sido identificadas normas de isenção dessa obrigação, a título de exemplo de experiências internacionais, destaca-se o material disponibilizado pela ICO[25], em seu site na Internet, sobre questionário de autoavaliação para verificação dos procedimentos de resposta a incidentes de segurança da informação da empresa.

Além disso, foi disponibilizado na web um passo a passo de como pequenas e médias empresas devem proceder para realizar a comunicação[26], inclusive atendendo o prazo de 72 (setenta e duas) horas.

Outro exemplo, cita-se a experiência de Luxemburgo[27] com a disponibilização de formulário simplificado e estruturado para comunicação de incidentes de segurança.

Encarregado

Em relação à nomeação do encarregado de proteção de dados, as experiências internacionais demonstram que, geralmente, a obrigação de indicá-lo está relacionada aos riscos e danos aos quais os titulares estão expostos.

Por exemplo, na União Europeia, o RGDP[28] dispõe que a designação de um encarregado é obrigatória nos seguintes casos:

a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

[25] ICO. "How well could you respond to a personal data breach?". Disponível em: https://ico.org.uk/for-organisations/sme-web-hub/checklists/how-well-could-you-respond-to-a-personal-data-breach/. Acesso em: 27/07/2021.
[26] ICO. 72 hours - how to respond to a personal data breach. Disponível em: https://ico.org.uk/for-organisations/sme-web-hub/72-hours-how-to-respond-to-a-personal-data-breach/. Acesso em 27/07/2021.
[27] CNPD. Formulaire de Notification des Violations de Données. Disponível em: https://cnpd.public.lu/fr/formulaires.html. Acesso em 27/07/2021.
[28] RGDP. Regulamento Geral sobre Proteção de Dados. Art. 37. Disponível em: https://gdprinfo.eu/pt-pt/pt-pt-article-37. Acesso em 27/07/2021.

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controle regular e sistemático dos titulares dos dados em grande escala; ou

c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9 e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.

Especificamente para pequenas e médias empresas, a União Europeia recomenda[29] a nomeação de um encarregado nos casos em que: (i) se processe dados pessoais para direcionar publicidade, por meio de motores de busca com base no comportamento online dos indivíduos, e (ii) se processe dados relacionados à genética e saúde para hospitais.

Em sentido parecido, em Portugal[30], as empresas, seja na qualidade de responsáveis pelos tratamentos, seja na de subcontratantes, só estão obrigadas a designar um encarregado se realizarem o tratamento de dados sensíveis ou de dados relativos a condenações penais e infrações, nos termos dos artigos 9º e 10º do RGDP, em larga escala ou se realizarem tratamentos em larga escala relativos ao controle regular e sistemático dos titulares dos dados.

Prazos diferenciados

Não foram identificadas experiências internacionais a respeito do tema.

3.2.1.5 Quais os objetivos da ação? Por que a intervenção regulatória é necessária?

O objetivo imediato da intervenção regulatória é atender ao comando do art. 55-J, XVIII da LGPD e editar norma específica, simplificando e diferenciando os procedimentos para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam se adequar à LGPD.

Constituem contornos dessa norma específica o compromisso de garantir o direito à proteção de dados pessoais dos titulares, o equilíbrio entre as regras constantes da LGPD e o porte

[29] Europeran Commision. Data protection – Better rules for small business. Disponível em: https://ec.europa.eu/justice/smedataprotect/index_en.htm. Acesso em 27/07/2021.
[30] CNPD. Obrigações Encarregado de Proteção de Dados. Disponível em: https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/. Acesso em: 27/07/2021.

das microempresas, das empresas de pequeno porte, das *startups*, e as pessoas físicas que tratam dados pessoais e demais entidades, pelo que se concluiu que deveriam compor esse grupo de agentes de tratamento, buscando incentivar a inovação e o desenvolvimento econômico.

Outro objetivo imediato é facilitar a adaptação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais à LGPD, promovendo sua conformidade com a lei e contribuindo para a disseminação da cultura de proteção de dados pessoais.

Especificamente no que se refere ao tema relacionado à conformidade das obrigações da LGPD pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, objetiva-se uma maneira desses agentes se adequarem à LGPD sem colocar em risco ou causar danos aos titulares.

3.2.1.6 Quais os grupos afetados?

A norma de aplicação da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais impacta todos os titulares de dados que se relacionam com esse grupo de agentes de tratamento. Diante disso, ao proceder o levantamento dos agentes econômicos, dos usuários dos serviços prestados e dos demais afetados pelo problema ora analisado, os grupos a seguir foram identificados como mais impactados:

i) agentes de tratamento de dados, em especial aqueles em que se enquadram as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais;

ii) titulares de dados pessoais;

iii) fabricantes de *softwares* de gestão e governança de dados;

iv) prestadores de serviço de consultoria;

Outros grupos identificados, como órgãos de pesquisa, órgãos públicos, agências reguladoras e imprensa poderão ser afetados, mas com impactos reduzidos ou na medida em que se relacionarem com microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

3.2.2 ANÁLISE DAS ALTERNATIVAS

3.2.2.1 Quais são as opções regulatórias consideradas pelo tema?

Como já citado neste relatório, o comando do art. 55-J, XVIII da LGPD definiu a competência da ANPD para editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam adequar-se à lei.

Nesse sentido, a análise de impacto regulatório considerou como uma opção a adoção de uma alternativa regulatória baseada no modelo de flexibilização das obrigações dispostas na LGPD em um normativo único, ou seja, todas as flexibilizações estariam consolidadas em uma resolução única endereçada exclusivamente para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

A segunda alternativa seria a adoção de modelo regulatório cuja simplificação de cada uma das obrigações da LGPD para esse grupo de agentes de tratamento sejam tratadas principalmente nas resoluções específicas de cada um dos temas que devem ser regulamentados pela ANPD, considerando, além do porte dos agentes, os riscos e danos que o tratamento de dados pode causar aos titulares.

No entanto, cabe destacar que ainda que a segunda alternativa venha a ser adotada, seria necessária a edição de um normativo para dispor sobre a definição do grupo de agentes de tratamento que poderão fazer jus às regras simplificadas.

Por fim, cabe salientar que, independentemente do modelo proposto, considera-se uma atuação da ANPD mais orientativa e educativa, por meio de guias, *templates*, *checklists* e formulários simplificados, para que esse grupo de agentes de tratamento se adequem à LGPD.

A seguir são analisadas as alternativas de modelos regulatórios para atender o comando do art. 55-J, XVIII da LGPD. Cabe destacar que as análises realizadas no próximo tópico se referem às possíveis simplificações e flexibilizações das obrigações evidenciadas, bem como à forma da abordagem dessas flexibilizações em resolução única ou em resolução específica.

3.2.2.2 Alternativa A – Adoção de modelo regulatório com simplificação e flexibilização das obrigações em uma resolução única

A primeira alternativa se refere a uma abordagem com a edição de uma resolução única que identifique as simplificações e flexibilizações das obrigações dispostas na LGPD para que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam se adequar à lei. Espera-se que essa alternativa seja capaz de inserir em um normativo único as flexibilizações das obrigações da LGPD evidenciadas durante a análise, de forma a endereçar soluções aos problemas identificados.

A seguir são realizadas as análises desta alternativa, seguindo a divisão das principais obrigações da LGPD.

Obrigações relacionadas aos direitos do titular

A definição das normas simplificadas referentes às obrigações relacionadas aos direitos dos titulares em resolução única a ser editada traria maior segurança jurídica às microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, tendo em vista que esse grupo de agentes já saberia como se adequar ao que se é esperado e como cumpri-las. Por outro lado, a definição da forma simplificada de cumprimento sem que sejam estabelecidas as regras gerais para todos os agentes de tratamento pode gerar um descompasso e insegurança jurídica aos demais. Além disso, a regulamentação do tema está prevista na Agenda Regulatória 2021-2022 da ANPD, já com previsão de estudo e endereçamento pela Autoridade.

De todo modo, seja em resolução única ou em específica, já é possível mapear as principais obrigações aqui tratadas. No geral, para atendimento dos direitos dos titulares, os agentes de tratamento devem adequar suas atividades internas em termos de forma de recebimento das requisições e forma de resposta; fluxos internos para tratamento das solicitações e definição de responsáveis; análise e escolha da opção para atendimento da requisição; e prazo de atendimento, sem prejuízo de outras aqui não listadas.

Independentemente da alternativa a ser escolhida, já é possível traçar algumas das alternativas para que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam cumprir com as principais obrigações decorrentes do exercício dos direitos dos titulares de dados de forma simplificada. Para isso, será analisada cada obrigação constante da LGPD separadamente.

Em seu art. 18, a LGPD prevê o direito de o titular dos dados pessoais obter do controlador ações e informações em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição. Contudo, a lei não dispõe sobre os meios em que essa requisição será operacionalizada, cabendo então à regulamentação fazê-lo.

No RGPD, o "pedido de acesso ao titular" previsto nos artigos 12 e 15 pode ser solicitado por telefone, pessoalmente ou por escrito, devendo a resposta ser feita pelo mesmo meio, exceto se o requerente solicitar por outra forma.

O contexto de pandemia evidenciou a importância da utilização de meios remotos e digitais para os mais diversos serviços, impulsando a transformação digital em organizações públicas e privadas. Assim, entende-se que devem ser prestigiados os meios remotos – eletrônicos, digitais e telefônicos – de comunicação entre os agentes de tratamento e os titulares de dados, de modo a facilitar a troca de informações entre eles.

Dessa forma, sugere-se que a norma deixe expressa a previsão da possibilidade de atendimento das requisições por meio eletrônico, telefônico ou impresso, a ser escolhido pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. Destaca-se, ainda, que essa previsão está em consonância com a experiência internacional.

Seja ela em resolução única ou específica, essa obrigação pode, desde já, ser determinada na presente regulamentação, pois não afeta a regulamentação específica posterior sobre o direito dos titulares de dados (momento no qual as disposições serão aprofundadas) e não restringe os direitos do titular, mas tão somente permite o direcionamento para o seu exercício, ao mesmo tempo que desonera esse grupo de agentes de tratamento.

No mesmo sentido, entende-se que o acesso pelo titular às informações sobre o tratamento de seus dados, disposto no art. 9º da LGPD, deveria poder ocorrer por meio eletrônico ou por qualquer outra forma, a fim de permitir o acesso facilitado entre esse grupo de agentes e o titular dos dados pessoais.

Sobre a obrigação de anonimizar, bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGDP quando solicitados pelo titular de dados, na forma do art. 18, inciso IV, da LGPD, cabe destacar que várias contribuições apresentadas na

Tomada de Subsídios nº 1/2021 apontaram pela complexidade desta obrigação, principalmente com relação à anonimização.

Segundo a LGPD, a anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Existem várias técnicas de anonimização[31], que podem variar de complexidade a depender de sua aplicabilidade e finalidade. No entanto, a implementação dessas técnicas necessita da realização de uma avaliação criteriosa, conforme disposto no código de prática[32] publicada pela autoridade de proteção de dados do Reino Unido.

Tendo em vista a baixa maturidade das microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais no que se refere à adequação à LGPD, entende-se como razoável flexibilizar essa obrigação, sem que isso implique na sua dispensa completa, que poderia restringir os direitos dos titulares de dados, mas deixando a cargo desse grupo de agentes a opção para atender à solicitação do titular de dados, permitindo, assim, uma diminuição de seus custos na adequação à LGPD.

Assim, observa-se que essa solução busca proporcionar um equilíbrio entre o atendimento do dispositivo legal com a garantia do direito do titular de anonimizar, bloquear ou eliminar dados desnecessários, ao mesmo tempo em que se permite um tratamento diferenciado às microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais.

Quanto à portabilidade dos dados do titular, prevista no art. 18, inciso V, da LGPD, cabe avaliar a possibilidade desse grupo de agentes ser dispensado dessa obrigação ou tê-la flexibilizada.

Por um lado, a portabilidade de dados é benéfica para o titular de dados, porque pode facilitar o livre fluxo informacional entre os agentes de tratamento, possibilitando o exercício do direito de escolha pelo consumidor – a sua autodeterminação informacional, além de favorecer a

[31] PDPC. Guide to Basic Data Anonymisation Techniques. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf. Acesso em 05/08/2021.
[32] ICO. Anonymisation: managing data protection risk code of practice. Disponível em: https://ico.org.uk/media/1061/anonymisation-code.pdf. Acesso em 05/08/2021.

concorrência no mercado, ao possibilitar que os dados sejam migrados para novos entrantes e, com isso, favorecer a competição.

Contudo, a portabilidade exige investimentos financeiros e tecnológicos de interoperabilidade que podem se revelar desproporcionais à capacidade econômica desse grupo de agentes de tratamento de dados.

Nesse sentido, o estudo[33] publicado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), dentre outros assuntos, trata da questão da portabilidade e interoperabilidade de dados. No estudo foi citado que a "portabilidade de dados prevista no RGDP impõe altos custos de conformidade", e que quando aplicado a empresas que não possuem posição dominante em um mercado, pode impedir a concorrência e, em última análise, prejudicar os consumidores. Diante disso, o estudo cita o artigo[34] de dois autores, Diker Vanberg e Ünve, que sugerem um regime de isenção para pequenas e médias empresas e empresas com uma pequena participação de mercado ou volume de negócios.

A título de exemplo do desafio de assegurar a interoperabilidade de dados, menciona-se o *Open Banking*, iniciativa conduzida pelo Banco Central nos termos da Resolução Conjunta nº 1/2020,[35] a qual dispõe sobre o direito ao compartilhamento de dados bancários. Para tanto, as instituições participantes devem disponibilizar interfaces dedicadas ao compartilhamento de dados e serviços, os quais devem ser representados em meio digital e processáveis por máquina, em formato livre de restrição quanto à sua utilização. Cabe salientar que as instituições financeiras geralmente possuem sistemas altamente desenvolvidos e, devido à complexidade do projeto, precisaram de prazo razoável para efetivar a implementação, o que, comparativamente ao grupo de agentes aqui estudados, mostra-se de altíssimo custo para realização e implementação.

[33] OCDE. Consumer Data Rights and Competition - Background note. Disponível em: https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf. Acesso em 05/08/2021.

[34] Diker Vanberg, A. e M. Ünver. "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?". Disponível em: https://arro.anglia.ac.uk/id/eprint/701565/1/Diker%20Vanberg_2017.pdf. Acesso em 06/08/2021.

[35] BACEN. Resolução Conjunta nº 1, de 04 de maio de 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v2_P.pdf. Acesso em 05/08/2021.

Nesse exemplo, o Banco Central estipulou que a adesão ao Open Banking era facultativa para as instituições financeiras de menor porte[36]:

> Somente as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central podem participar do ecossistema do Open Banking. Entre esse universo de instituições, no entanto, **a regulamentação prevê participantes obrigatórios e voluntários, a depender do porte da instituição e do dado ou serviço que está sendo compartilhado**. Os maiores bancos, por exemplo, são participantes obrigatórios do Open Banking para o compartilhamento de dados. [grifamos]

Diante disso, dispensar as microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais da obrigação de conferir o direito à portabilidade, em um primeiro momento de estabelecimento de normas que simplifiquem obrigações e possibilitem uma adequação à LGPD enquanto não são estabelecidos parâmetros razoáveis que tornem essa prerrogativa viável, parece ser razoável, sem prejuízo de nova avaliação em momento de normatização do tema pela ANPD.

Quanto à obrigação de envio de declaração a que se refere o art. 19, inciso II, da LGPD, entende-se que microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais podem ser dispensadas do envio da declaração completa, sendo suficiente o formato simplificado, já previsto no inciso I do mesmo artigo da lei.

O art. 19 da lei trata da confirmação de existência ou o acesso a dados pessoais, mediante solicitação do titular, nos seguintes termos:

> 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 15 (quinze) dias, contado da data do requerimento do titular. [grifamos]

Observa-se que os incisos I e II do art. 19 propõem duas alternativas para atender o comando do caput do artigo, sendo estes por meio de formato simplificado ou de declaração clara e completa.

[36] BACEN. Open Banking: instituições participantes. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/openbanking. Acesso em: 16/08/2021.

Como já citado nesta análise, as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possuem dificuldades de adequação à LGPD, tanto que o art. 55-J, XVIII da referida lei estabeleceu que compete à ANPD editar regras simplificadas para esse grupo de agentes.

Dessa forma, entende-se conveniente já indicar expressamente que o atendimento do art. 19 da LGPD possa ocorrer por meio de formato simplificado, tendo em vista que isso diminui a complexidade do atendimento do dispositivo legal e, ao mesmo tempo, preserva o direito do titular de dados de receber a declaração sobre os seus dados.

Por fim, no intuito de fomentar o apoio das entidades de representação da atividade empresarial relacionadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais nas questões referentes aos direitos dos titulares – ponto trazido em algumas das contribuições da Tomada de Subsídios nº 1/2021, sugere-se a inclusão de uma previsão no sentido de que tais entidades possam prestar assessoria e auxiliar na negociação, na mediação e na conciliação de reclamações apresentadas por titulares de dados.

No caso, a justificativa para o estabelecimento dessa possibilidade é o auxílio que essas entidades podem prestar a esse grupo de agentes de tratamento, que não possuem uma alta conformidade com as obrigações da LGPD. Com isso, espera-se que o cumprimento e a adaptação tanto quanto à LGPD quanto à norma a ser editada pela ANPD possam ser realizadas com menores custos a esse grupo de agentes de tratamento, bem como que se aumente o número de empresas adequadas ao sistema de proteção de dados, já que, com custos menores, a tendência é que mais empresas consigam se adequar com menos dificuldades.

Além disso, o estabelecimento dessa previsão não restringe ou diminui os direitos dos titulares de dados, mas, sim, tende a beneficiá-los com o maior cumprimento das obrigações pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, seja em resolução única, seja em resolução específica.

Registro das Atividades de Tratamento

O registro das atividades de tratamento está previsto no art. 37 da LGPD, que determina que "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse". A lei, portanto, exige que

esses agentes mantenham um inventário das informações relacionadas às operações de tratamento de dados que realizarem, desde a coleta do dado até sua exclusão.

Contudo, a LGPD não fornece os contornos desse registro, nem dita quais elementos ele deve conter, diferente do RGPD, por exemplo, que prevê as informações que devem ser registradas tanto pelo controlador, quanto pelo operador. Ademais, a LGPD não prevê exceções ao dever de registro, de modo que, a princípio, ele se aplica a todos os agentes de tratamento, da mesma forma.

O RGPD, ao contrário, informa que empresas que possuam menos de 250 funcionários não precisam manter registros do procedimento de tratamento de dados, a não ser quando os tratamentos realizados tenham alto potencial de resultar em um risco para os direitos e liberdades dos titulares, quando forem tratamentos habituais ou quando incluírem dados de categoria especial ou dados relacionados a ofensas e condenações criminais.

Cabe à regulamentação brasileira, portanto, indicar os critérios que devem ser adotados pelo controlador e operador para o registro das atividades de tratamento de dados, bem como eventual flexibilização no dever de registro. No entanto, tendo em vista a falta de previsão de sua regulamentação pela Agenda Regulatória 2021-2022, a flexibilização das obrigações sobre o tema em resolução única promoveria maior segurança jurídica às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. Por sua vez, se a edição de resolução específica pode permitir o aprofundamento do tema, aguardar a sua edição sem que haja expectativa quanto ao seu endereçamento pela ANPD pode onerar de forma desproporcional esse grupo de agentes.

Diante disso, cabe endereçar, aqui, quais seriam as flexibilizações possíveis em resolução única.

Seguindo a lógica da experiência internacional, as alternativas para a flexibilização do dever de registro das operações de tratamento podem recair sobre os critérios de porte e capacidade econômica do agente de tratamento e ao risco atrelado à atividade de tratamento de dados.

Iniciando pelo critério do porte econômico, no caso das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, o simples registro das atividades de tratamento de dados pessoais já representa, por si só, um desafio, eis que a atividade

de registro e manutenção das informações envolve conhecimento jurídico e técnico, além de custo financeiro, considerando que se trata de uma atividade contínua a ser desempenhada.

Manter o registro das atividades de tratamento, por outro lado, é importante para conferir segurança jurídica tanto a esse grupo de agentes de tratamento, quanto ao titular de dados, além de atender aos comandos da transparência, de *accountability* e do acesso aos dados pelo titular. Ainda que não mantidos os registros das atividades de tratamento de dados pessoais, é importante que as organizações conheçam o ciclo de vida dos dados, como e quais dados coleta e que atividades de tratamento realizam.

Considerando, no entanto, o pequeno volume de dados envolvido nas atividades das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, o registro torna-se uma exigência desproporcional em razão do custo envolvido, seja em termos de capacitação jurídica e técnica, seja em termos financeiros para manutenção contínua dessa atividade.

Com efeito, trazer exigências cujo investimento por esse grupo de agentes não é razoável face ao benefício obtido e à possibilidade de afetar a capacidade efetiva de o agente atuar em conformidade com a previsão legal, o que não é desejável. Além disso, sem esse investimento dificilmente o comando legal pode ser cumprido, dado que, em geral, as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais não sabem como registrar as atividades de tratamento, tendo assim que recorrer a consultorias externas ou, eventualmente, deixar as questões de privacidade e proteção de dados em segundo plano. De fato, a manutenção dos registros de atividades de tratamento requer uma estrutura organizacional mais robusta, com programas de governança já estruturados, processos internos bem definidos, e políticas e capacitação específicas para proteção de dados, o que não condiz com a desse grupo de agentes.

Assim, a dispensa da obrigação de manutenção de registros das operações de tratamento de dados pessoais constante do art. 37 da LGPD para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais é uma alternativa que se mostra viável de acordo com a realidade e a capacidade limitada dos referidos agentes, e não impõe ônus desproporcional, que pode inviabilizar a sua atuação em conformidade com a regulamentação da LGPD e com seu próprio desenvolvimento econômico.

Cabe destacar, ademais, que o critério de risco também está sendo levado em consideração neste contexto, na medida em que a obrigação ora flexibilizada não se aplica a esse grupo de agentes de tratamento que realizem tratamento de alto risco para os titulares. Portanto, tanto o critério do porte econômico, quanto o critério do risco envolvido, estão sendo levados em consideração nessa alternativa regulatória.

Relatório de Impacto à Proteção de Dados Pessoais

O relatório de impacto à proteção de dados está previsto no art. 5º, inciso XVII, da LGPD, como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Trata-se, portanto, de um relatório elaborado para avaliação periódica de riscos de uma atividade de tratamento de dados que pode gerar prejuízos ao titular. Nesse sentido, o que vai determinar a necessidade de sua elaboração não é a natureza do agente de tratamento, mas, sim, o alto risco potencialmente envolvido na atividade de tratamento de dados.

O tema está previsto no item 7 da Agenda Regulatória para o biênio 2021-2022 da ANPD, sendo que seu processo de regulamentação já foi iniciado, conforme relatório de acompanhamento da agenda.[37]

Espera-se que o normativo a ser editado sobre o tema defina as metodologias que a ANPD irá adotar para estabelecer as operações de tratamento de dados de alto risco que ensejarão a necessidade de elaboração de um relatório de impacto à proteção de dados.

Se por um lado a inclusão da simplificação em norma única favorece esse grupo de agentes de tratamento ao desonerá-los, por outro, conferir um regime diferenciado às microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais, antes da discussão propriamente dita do assunto no âmbito de seu próprio processo de regulamentação não se mostra eficiente, considerando que o agente de tratamento não é o principal elemento nesta análise, mas, sim, o risco envolvido para o titular de dados.

[37] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022

Assim, ainda que se conclua pela inclusão do tema em resolução única, entende-se que não seria possível já prever as flexibilizações para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Comunicação de Incidentes de Segurança

O art. 48 da LGPD dispõe que o controlador deve comunicar à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Neste sentido, o item 6 da Agenda Regulatória 2021-2022 da ANPD tem como escopo regulamentar essa obrigação, que já teve o seu processo de regulamentação iniciado, conforme relatório de acompanhamento da agenda.[38]

No âmbito da regulamentação, espera-se que sejam realizados estudos sobre as vulnerabilidades no tratamento de dados que possam acarretar riscos ou danos relevantes aos titulares, bem como sobre uma metodologia para cálculo do índice de gravidade de incidentes de segurança, dentre outros fatores.

Um dos principais argumentos para antecipar o tratamento do assunto em resolução única diz respeito aos custos relacionados à comunicação de incidentes de segurança. Nesse sentido, cabe salientar que na Tomada de Subsídios nº 1/2021 foram apresentadas contribuições no sentido de que os custos de implementação de um projeto de proteção de dados, incluindo a obrigação na íntegra de comunicação de incidentes disposta na LGPD são elevados, tanto sob a ótica financeira quanto sob a ótica de capital humano. Assim, eventuais flexibilizações poderiam diminuir custos para o cumprimento das obrigações dispostas pela LGPD pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Por outro lado, assim como no caso do relatório de impacto, a norma específica poderá estabelecer todas as previsões necessárias para endereçar o assunto, bem como espera-se que o processo de regulamentação aprofunde o estudo do tema de maneira adequada.

Assim, diante da complexidade do tema, sugere-se que, caso incluída em eventual resolução única, a previsão seja de possibilidade de edição de um modelo de comunicação simplificada a ser

[38] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022

disponibilizado pela ANPD, tendo em vista já existir um modelo geral disponível no site da Autoridade.

Destaca-se que um procedimento simplificado de comunicação de incidentes não implica em uma restrição aos direitos dos titulares de dados, tendo em vista que a premissa aqui adotada é que a comunicação ainda será realizada e os titulares de dados ainda serão informados, mas com um formulário de comunicação que gere um ônus menor às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Encarregado

A LGPD determina a obrigação de indicação de encarregado nos termos do art. 41:

> *Art. 41. O controlador deverá indicar 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 controlador.*
> *§ 2º As atividades do encarregado consistem em:*
> *I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*
> *II - receber comunicações da autoridade nacional 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 - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.*
> *§ 3º A autoridade nacional 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.*

O tema foi incluído na Agenda Regulatória 2021-2022 e não teve o seu processo de regulamentação iniciado até o momento.

Segundo as contribuições da Tomada de Subsídios nº 1/2021, como o levantamento da CNI,[39] o custo anual de contratação de um encarregado de dados foi estimado em R$ 360.000,00, o

[39] Pequenas empresas têm tratamento especial na LGPD na Europa e Austrália. Disponível em: https://noticias.portaldaindustria.com.br/noticias/economia/pequenas-empresas-tem-tratamento-especial-na-lgpd-na-europa-e-australia/ Acesso em 21/07/2021.

que equivale, praticamente, ao teto do faturamento das microempresas e empresas de pequeno porte nos termos da Lei nº 123/2006.

Sobre esse ponto, apenas a título de exemplo, os salários de um encarregado na Europa atingiam a média anual de 88.000 euros em maio de 2019, considerando as 500.000 empresas que já haviam nomeado seus encarregados.[40]

Dessa forma, considera-se possível evidência de dificuldade de recursos financeiros e humanos para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais indiquem o encarregado de dados. No entanto, cabe destacar que aqueles agentes que realizarem tratamento de alto risco para os titulares devem indicar o encarregado com objetivo de reduzir os riscos de tratamentos inadequados de acordo com a LGPD, bem como evitar incidentes de segurança. Cabe lembrar que o tema 1 deste relatório de AIR já abordou as questões relacionadas à definição de tratamento de alto risco para os titulares de dados.

Além disso, entende-se inviável que o microempreendedor individual contrate um encarregado de dados, mesmo que realize tratamento de alto risco, tendo em vista que são empreendedores que trabalham por conta própria com receita bruta anual igual ou inferior a R$ 81.000,00 (oitenta e um mil reais), nos termos do art. 18-A da Lei Complementar nº 123/2006.

Ademais, os microempreendedores geralmente são profissionais que realizam tratamento de dados pessoais simplificados, como por exemplo, coleta e armazenamento de dados pessoais. Para tal, utilizam *softwares* e plataformas, inclusive de serviços em nuvem, fornecidas por empresas globais que baseiam o desenvolvimento de seus produtos em recomendações internacionais de segurança e de boas práticas.

Caso a flexibilização do cumprimento dessas obrigações seja feita em normativo único, entende-se que seriam enfrentadas dificuldades similares àquelas elencadas nos casos do relatório de impacto à proteção de dados pessoais e de comunicação de incidentes de segurança, ou seja, seria necessário se estabelecer flexibilizações antes das definições gerais sobre o tema.

[40] INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP). Approaching One Year of GDPR Anniversary, IAPP Reports Estimated 500,000 Organizations Registered DPOs In Europe. Disponível em https://iapp.org/about/approaching-one-year-gdpr-anniversary-iapp-reports-estimated-500000-organizations-registered-dpos-in-europe/. Acesso em: 29/07/2021.

No entanto, tendo em vista o alto custo que a obrigação de indicação de um encarregado impõe, sugere-se que no caso de inclusão do tema em resolução única seja prevista a dispensa da sua indicação por microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais. No caso, isso não implicaria inexistência de canais de comunicação entre esse grupo de agentes de tratamento e os titulares de dados, mas tão somente a possibilidade de desempenho dessa função de formas alternativas, de forma que os direitos dos titulares de dados seriam preservados.

Prazos diferenciados

Com relação à adoção de prazos diferenciados para atendimento das obrigações da LGPD para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, entende-se que, diante da baixa maturidade e recursos limitados desse grupo de agentes de tratamento, o cumprimento dos prazos definidos pela ANDP pode se tornar outra barreira para a inserção destes agentes de tratamento no arcabouço regulatório de proteção de dados.

Nessa linha, o art. 55-J, XVIII, da LGPD, que trata das normas, orientações e procedimentos simplificados para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, define expressamente a possiblidade de prazos diferenciados para esses agentes.

Cabe esclarecer que, com exceção do art. 19, II, da LGPD, a lei endereça os tratamentos de prazos para a regulamentação específica, que definirá os prazos mais apropriados.

Se por um lado uma previsão relacionada aos prazos em normativo único encontra dificuldades relacionadas à inexistência de definição dos prazos para cumprimento de obrigações para todos os agentes, por outro a inclusão de previsão sobre o tema tende a gerar segurança jurídica para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. Caso essa previsão seja incluída em normas específicas, os benefícios esperados são os mesmos, porém deixando esse grupo de agentes sem informações quanto à flexibilização em relação ao tema.

Assim, independentemente da alternativa regulatória que venha a ser adotada, entende-se que o modelo com uma flexibilização de prazos com abordagem de contagem em dobro possibilitará que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que

tratam dados pessoais possam adequar-se à LGPD sem causar danos ou colocar em risco os direitos dos titulares de dados.

Resumo da análise da alternativa A

Grupos afetados	Desafios	Benefícios
ANPD	Definição de dispensas e flexibilizações de obrigações para um grupo específico sem antes definir o modelo regulatório geral das obrigações previstas na LGPD. Risco de elevar o número de processos sancionatórios e, consequentemente, longa duração das decisões desses processos, caso não sejam identificadas todas as obrigações passíveis de flexibilização ou dispensa. Risco de percepção social de pouca efetividade das ações da ANPD, caso não sejam identificadas todas as obrigações passíveis de flexibilização ou dispensa.	Maior rapidez na publicação das regras de flexibilização ou de dispensa das obrigações.
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Risco de aumento de despesas para atendimento das obrigações, caso não sejam identificadas todas as obrigações passíveis de flexibilização ou dispensa. Risco de reduzir o número de agentes desse grupo, caso não sejam identificadas todas as obrigações passíveis de flexibilização. Risco de reduzir investimentos nos negócios principais destes agentes, incluindo a inovação, caso não sejam identificadas todas as obrigações passíveis de flexibilização ou dispensa.	Consolidação das flexibilizações das obrigações em instrumento normativo único. Maior rapidez na efetividade da flexibilização ou de dispensa da obrigação.
Titulares de dados pessoais	Risco de elevar as ameaças aos direitos dos titulares, caso ocorram dispensas ou flexibilizações equivocadas das obrigações.	Não foram identificados benefícios.
Fabricantes de *softwares* e plataformas	Risco de redução de demandas proporcionada por esse grupo de agentes. Os agentes ficam menos propensos a fazer investimentos, já que existe o risco de que não se atinja a conformidade.	Não foram identificados benefícios.
Prestadores de consultoria	Risco de redução de demandas proporcionada por esse grupo de agentes. Esses agentes ficam menos propensos a fazer investimentos, já que existe o risco de que não se atinja a conformidade.	Não foram identificados benefícios.

3.2.2.3 Alternativa B – Adoção de modelo regulatório de simplificação e flexibilização das obrigações em resoluções específicas

Com a adoção do modelo regulatório de simplificação e flexibilização das obrigações em resoluções específicas referentes à cada obrigação, espera-se que os temas sejam tratados de forma completa, respeitando as suas respectivas complexidades, sem o estabelecimento de regras antecipadas apenas para um grupo de agentes.

No entanto, mesmo que essa opção seja adotada, destaca-se que será necessária a edição de uma norma para definir quais agentes de tratamento fazem jus aos regimes simplificados que serão previstos nas normas específicas. A seguir são feitas as análises dessa alternativa, seguindo a divisão das principais obrigações da LGPD.

Das obrigações relacionadas aos direitos do titular

A regulamentação dos direitos dos titulares de dados pessoais consta do item 4 da Agenda Regulatória da ANPD para o biênio 2021-2022, cujo início do processo regulatório está previsto para o 1º semestre de 2022.

Com isso, tem-se que a flexibilização das obrigações referentes aos direitos dos titulares a serem cumpridas pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, caso seja determinada apenas na regulamentação específica, seria definida somente a partir do próximo ano.

Tal cenário pode gerar insegurança jurídica quanto ao cumprimento das obrigações por esse grupo de agentes, tendo em vista não disporem de tantos instrumentos e capacitação técnica para agirem em conformidade com a LGPD, necessitando, assim, de orientações mais céleres e tempestivas.

Por outro lado, a previsão de regime simplificado em norma específica possibilita um aprofundamento do tema pela ANPD, de forma que a flexibilização poderá englobar um número maior de aspectos relacionados às obrigações do encarregado para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Do Registro das Atividades de Tratamento

A regulamentação do registro das atividades de tratamento não foi prevista como uma das atividades normativas a serem desempenhadas pela ANPD pelos próximos 2 (dois) anos conforme a Agenda Regulatória 2021-2022.

Sem prejuízo de eventual inclusão desse tema na Agenda 2021-2022 em caso de eventual alteração ou inclusão na próxima agenda que venha a ser publicada, a simplificação do tema para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais em resolução específica pode onerar esse grupo de empresas de forma incompatível com o faturamento por ele auferido. Como dito anteriormente, o investimento envolvido na atividade de registro e manutenção de informações de tratamento de dados é alto para esse grupo de agentes de tratamento, dado o pequeno volume de dados com os quais trabalham, mostrando-se assim uma medida desproporcional.

Por outro lado, a alternativa de flexibilizar a obrigação de realizar o registro em uma resolução específica sobre a matéria pode permitir um estudo mais aprofundado do tema.

Do Relatório de Impacto à Proteção de Dados Pessoais

O relatório de impacto à proteção de dados é um dos temas prioritários e previstos para edição de regulamentação específica pela ANPD, conforme prevê o item 7 da Agenda Regulatória para o biênio 2021-2022 e cujo processo de regulamentação já foi iniciado, nos termos do relatório de acompanhamento da agenda regulatória.[41] Assim, espera-se que as metodologias e os critérios a serem adotados pela ANPD para estabelecer quais serão as operações de tratamento de dados consideradas de alto risco e que, portanto, ensejarão a necessidade de elaboração de um relatório de impacto à proteção de dados, sejam determinadas no âmbito da regulação específica.

Se por um lado a não inclusão de normas diferenciadas sobre o relatório de impacto à proteção de dados para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais pode gerar insegurança para esse grupo, cabe argumentar que a sua obrigatoriedade de elaboração advém da natureza da atividade de tratamento desenvolvida e de sua potencial violação aos direitos dos titulares de dados e que espera-se que a resolução de regime simplificado para esse grupo de agentes não se aplique aos agentes de tratamento que realizem

[41] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022

tratamento de alto risco. Assim, pode-se argumentar que os destinatários da norma não seriam de fato prejudicados com um normativo específico, tendo em vista que essa obrigação não se destinaria a eles.

Contudo, embora o que determine a necessidade de elaboração de um relatório de impacto não seja a natureza do agente de tratamento, é certo que a sua forma pode ser diferenciada para esse grupo de agentes de tratamento que possui menor capacidade de se estruturar para apresentar um relatório completo e detalhado. Assim, podem as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais dispor de um instrumento simplificado para elaboração do relatório de impacto.

Da Comunicação de Incidentes de Segurança

Como já mencionado neste relatório, o item 6 da Agenda Regulatória 2021/2022 da ANPD trata do tema, cuja regulamentação já foi iniciada pela ANPD, conforme relatório de acompanhamento da Agenda.[42]

Nesse sentido, nota-se que já existe previsão de edição de normativo específico sobre o assunto, que pode incluir todas as previsões a serem simplificadas a partir de uma análise mais aprofundada, podendo de fato identificar as vulnerabilidades no tratamento de dados que possam acarretar riscos ou danos relevantes aos titulares, bem como estabelecer uma metodologia para cálculo do índice de gravidade de incidentes de segurança. A partir desses estudos, seria possível para ANPD ter maturidade suficiente para avaliar as simplificações ou as flexibilizações das obrigações.

Por outro lado, a ausência de qualquer sinalização de eventual flexibilização a ser estabelecida pela ANPD pode gerar um aumento de custo às microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, além de gerar insegurança jurídica. Outro aspecto é que esse grupo de agentes pode realizar uma adequação sobre o assunto para, a partir de edição de norma específica, ter que realizar uma adaptação.

Do Encarregado

[42] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022

A Agenda Regulatória da ANPD para o biênio 2021/2022 prevê a regulamentação do tema, com previsão para início do seu processo de regulamentação no primeiro semestre de 2022.

Identifica-se, assim, que o primeiro prejuízo em se estabelecer o regime simplificado para essa obrigação para as microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais é o tempo que se levaria até a publicação da versão final da norma sobre o assunto. Nesse sentido, cabe destacar que este relatório já elencou as dificuldades de recursos financeiros e humanos para que esse grupo de agentes arquem com a obrigação de indicar o encarregado de dados.

Por outro lado, a simplificação em resolução específica poderá aprofundar o estudo do tema e eventualmente realizar novas flexibilizações que beneficiem as microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais.

Dos prazos diferenciados

Sobre a adoção de prazos diferenciados para atendimento das obrigações da LGPD para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, conforme já esclarecido neste relatório, entende-se que, diante da baixa maturidade em relação ao cumprimento da LGPD e dos recursos limitados desse grupo de agentes, o cumprimento dos prazos definidos pela ANDP pode ser tornar outra barreira para a inserção desses agentes no arcabouço regulatório de proteção de dados.

Dessa forma, entende-se que, independentemente da alternativa regulatória adotada, a adoção de uma flexibilização quanto aos prazos – sugerindo-se aqui a sua contagem em dobro – possibilitará que esse grupo possa se adequar à LGPD sem causar danos ou colocar em risco os direitos dos titulares de dados.

A definição relacionada aos prazos em resoluções específicas permitirá que esse grupo de agentes saiba, de fato, qual é o prazo esperado para o cumprimento das obrigações, conferindo, assim, maior segurança jurídica. Por outro lado, a espera para essa definição em resoluções específicas deixará as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais sem informações sobre o tema, gerando, assim, insegurança jurídica.

Resumo da análise da alternativa B

Grupos afetados	Desafios	Benefícios
ANPD	Maior demora na definição das regras de dispensa e flexibilização das obrigações para agentes de tratamento de pequeno porte. Percepção social de demora na efetividade das ações regulatórias da ANPD.	Maior maturidade na análise da dispensa ou da flexibilização das obrigações. Realização dos estudos de dispensa e flexibilização tendo maior conhecimento e maturidade quanto à obrigação geral a todos os agentes. Oportunidade de maior eficácia nos resultados regulatórios esperados.
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Maior demora na efetividade das regras de flexibilizações ou de dispensa das obrigações	Maior discussão sobre a matéria a ser tratada no normativo específico. Oportunidade de maior eficácia e efetividade das flexibilizações ou de dispensas das obrigações.
Titulares de dados pessoais	Não foram identificados problemas.	Oportunidade de reduzir as ameaças aos direitos dos titulares, caso as dispensas ou flexibilizações das obrigações sejam mais eficazes.
Fabricantes de *softwares* e plataformas	Não foram identificados problemas.	Oportunidade de aumento de demandas proporcionada pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.
Prestadores de consultoria	Não foram identificados problemas.	Oportunidade de aumento de demandas proporcionada pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

3.2.3 CONCLUSÃO E ALTERNATIVA SUGERIDA

3.2.3.1 Qual a conclusão da análise realizada?

Considerando as alternativas apresentadas como solução para os problemas relacionados à simplificação ou à flexibilização das obrigações da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, identificou-se que, em razão dos desafios e benefícios elencados para cada um dos grupos afetados, que a **Alternativa A** é a mais adequada para endereçar o tema.

Isso porque a edição de uma norma com a definição do conceito do grupo de agentes de tratamento aos quais a norma se aplicará e dos critérios de aplicação, bem como o adiantamento

da flexibilização em relação a algumas obrigações identificadas como passíveis de flexibilização no presente momento e o estabelecimento de formas diferenciadas de cumprimento de outras se mostra como a opção mais adequada para as microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, sem prejudicar os direitos dos titulares de dados.

No entanto, é preciso reconhecer que as flexibilizações relacionadas às obrigações mais complexas precisam de análise mais profunda, e que ocorrerão, portando, no âmbito dos projetos de elaboração das resoluções específicas.

Dessa forma, a opção pela alternativa A parcialmente conjugada com a alternativa B permite o atendimento do disposto no art. 55-J, XVIII, da LGPD, com a publicação de resolução que defina o grupo de agentes endereçados pela norma, considerando o porte das empresas e o tratamento de alto risco aos titulares de dados, e permite a inserção de algumas flexibilizações ou simplificações de obrigações consideradas evidentes. Ao mesmo tempo, essa opção possibilita que outras flexibilizações sejam avaliadas na execução de projetos de regulamentação de temas específicos, no qual espera-se que já se tenha maior maturidade sobre os assuntos a serem regulados.

3.2.3.2 Como será operacionalizada a alternativa sugerida?

Sobre a operacionalização da alternativa A parcialmente conjugada com a alternativa B, sugere-se que a ANPD adote uma atuação em duas frentes: i) elaboração de guias, frameworks, *templates* e formulários simplificados para apoiar a disseminação da cultura de proteção de dados, bem como disseminar o conhecimento da LGPD e ii) publicação de resolução para definição do conceito dos agentes de tratamento aos quais a norma se aplica, bem como inclusão na referida norma de algumas das flexibilizações das obrigações dispostas na LGPD, sem prejuízo de novas previsões em normas específicas.

Sobre o primeiro item, a ANPD já vem atuando de forma orientativa, com publicações de documentos com o objetivo de disseminação do conhecimento sobre a proteção de dados, tendo como base a LGPD. A título exemplificativo, tem-se a publicação do "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado",[43] que buscou estabelecer diretrizes não-vinculantes aos agentes de tratamento e explicar quem pode exercer a

[43] Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado. Acesso em 30/07/2021.

função do controlador, do operador e do encarregado; as definições legais; os respectivos regimes de responsabilidade; casos concretos que exemplificam as explicações da ANPD e as perguntas frequentes sobre o assunto.

Quanto à flexibilização das obrigações, propõe-se a seguinte abordagem na minuta da resolução a partir das análises feitas e das justificativas para sugestões de abordagens ao longo dos estudos das alternativas do tópico anterior.

Das obrigações relacionadas aos direitos do titular

Em relação às obrigações relacionadas aos direitos do titular, propõe-se que as requisições dos titulares de dados pessoais descritas no art. 18 da LGPD possam ser atendidas por meio eletrônico, telefônico ou impresso, deixando a cargo das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais a escolha pelo meio que lhe for mais conveniente. Essa alternativa não restringe o direito do titular, mas direciona a forma pela qual ele poderá ser exercido, ao mesmo tempo que não onera em demasia esse grupo de agentes de tratamento.

Pelo mesmo motivo, sugere-se que quando for solicitado pelo titular de dados, na forma do art. 18, inciso IV, da LGPD, as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais tenham a faculdade de optar por anonimizar, bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGDP.

No que tange à portabilidade dos dados do titular, conforme previsto no art. 18, inciso V, da LGPD, recomenda-se que esse grupo de agentes seja dispensado dessa obrigação, também em razão da onerosidade da medida, que não faz jus ao benefício do titular em relação ao custo envolvido para obtê-lo.

Quanto à declaração a que se refere o art. 19, inciso II, da LGPD, entendeu-se que as microempresas, empresas de pequeno porte, *startup*s e pessoas físicas que tratam dados pessoais podem ser dispensadas do envio da declaração completa, sendo suficiente a adoção de formato simplificado, já previsto no inciso I do mesmo artigo da lei.

Já quanto ao acesso pelo titular às informações sobre o tratamento de seus dados, disposto no art. 9º da LGPD, sugere-se que possa ocorrer por meio eletrônico ou por qualquer outra forma, a fim de permitir o acesso facilitado entre as microempresas, empresas de pequeno porte, startups

e pessoas físicas que tratam dados pessoais e o titular dos dados pessoais, ao mesmo tempo que não implica aumento de despesas para esse grupo de agentes de tratamento.

Por fim, no intuito de fomentar o apoio das entidades de representação da atividade empresarial relacionadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais nas questões referentes aos direitos dos titulares, sugere-se que elas possam prestar assessoria e auxiliar na negociação, na mediação e na conciliação de reclamações apresentadas por titulares de dados, incluindo aquelas que realizem tratamento de alto risco para os titulares.

Do Registro das Atividades de Tratamento

Com relação ao registro das atividades de tratamento, previsto no do art. 37 da LGPD, sugere-se que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais que não realizem tratamento de dados de alto risco para os titulares, sejam dispensadas da obrigação de manutenção de registros das operações de tratamento de dados pessoais dado o pequeno volume de dados envolvido nas atividades desses agentes.

Do Relatório de Impacto à Proteção de Dados Pessoais

Em relação ao relatório de impacto à proteção de dados pessoais, entende-se ser suficiente a inclusão de previsão de apresentação de um relatório de forma simplificada pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, cujo modelo será definido em resolução específica sobre o assunto quando houver tal exigência, tendo em vista que a ANPD já estuda a elaboração de uma norma sobre o tema. Isso permitirá o amadurecimento da matéria e uma melhor avaliação sobre os critérios de simplificação que poderão ser adotados pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, sem prejuízo do risco envolvido para os direitos dos titulares de dados.

Ainda que não definido o formato simplificado, a proposta não se mostra inócua ou irrelevante, pois acena positivamente para esse grupo de agentes, no sentido de que não precisarão investir de maneira desproporcional à sua capacidade econômica para se adequar aos termos da LGPD. Confere, assim, uma sinalização positiva para que, quando o assunto for regulamentado, sejam avaliadas e levadas em consideração as possibilidades de simplificação do modelo, para viabilizar a devida conformidade por esses agentes.

Da Comunicação dos Incidentes de Segurança

Diante do que já foi demonstrado neste relatório, sugere-se que a simplificação relacionada à obrigação de comunicar um incidente de segurança seja tratada em resolução específica. No caso, há previsão de edição de norma específica sobre o tema, que já é estudado de forma pormenorizada pela ANPD, nos termos da Agenda Regulatória 2021-2022, conforme pode ser observado no relatório de acompanhamento da Agenda[44]

Apesar disso, sugere-se que seja antecipada a previsão da possibilidade de flexibilização ou de adoção de procedimento simplificado de comunicação de incidente de segurança para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, a fim de que o assunto possa ser avaliado no momento oportuno, ao tempo em que se sinaliza a esse grupo de agentes a possibilidade de que regras diferenciadas venham a ser editadas sobre o assunto, tendo em vista as preocupações apresentadas ao longo da Tomada de Subsídios.

Do Encarregado

Diante das restrições financeiras e de pessoal, entende-se que destacar uma pessoa para exercer a função de encarregado no âmbito de uma microempresa, empresa de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais não é necessário para os fins do art. 41 da LGPD, cujo papel pode ser exercido por algum integrante da empresa, sem necessidade de indicação específica.

Tal dispensa está em consonância com o previsto no § 3º do art. 41 da LGPD, que dispõe que:

> § 3º A autoridade nacional 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.

Além disso, sugere-se que para o microempreendedor individual e para a pessoa física que trata dados pessoais a dispensa de indicação ocorra mesmo que eles realizem tratamento de alto risco para os titulares, já que essa categoria se resume a uma única pessoa que deverá adotar todas

[44] Nota Técnica nº 23/2021/CGN/ANPD – Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022

as medidas relacionadas à proteção de dados pessoais dentro da empresa, concentrando em si os papéis de controlador e encarregado.

Por fim, propõe-se que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais que não indicarem um encarregado tenham a obrigação de disponibilizar um canal de comunicação com o titular de dados, a fim de se garantir um meio em que possam ser recebidas as reclamações e feitas as comunicações com os titulares de dados pessoais. Dessa forma, preserva-se o direito do titular de manter um contato direito com esse grupo de agentes de tratamento, sem que isso os onere de forma desproporcional.

Dos prazos diferenciados

Quanto aos prazos diferenciados, sugere-se pela abordagem de concessão de prazo contado em dobro em relação ao concedido a outros agentes de tratamento nos seguintes casos:

a) no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, parágrafos 3º e 5º, e no art. 19 da LGPD, nos termos da resolução específica;
b) na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da resolução específica;
c) em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

Além disso, os prazos em dobro não especificados na proposta para esse grupo de agentes de tratamento serão determinados por resoluções específicas.

Assim, preservam-se os direitos dos titulares ao mesmo tempo que se diminuem a complexidade e os custos de obrigações para as microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais.

3.2.3.3 Como a alternativa sugerida será monitorada?

Sobre o monitoramento da alternativa A, ressalta-se que o monitoramento da efetividade da adaptação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais às obrigações dispostas na LGPD será realizado por meio do

acompanhamento das atividades de monitoramento e fiscalização desempenhadas pela Coordenação-Geral de Fiscalização, bem como por meio da elaboração dos relatórios anuais de gestão da ANPD. No caso, será possível aferir se as reclamações sobre esses agentes advêm da não conformidade das obrigações dispostas na LGPD.

Nesse sentido, sugere-se acompanhar a quantidade de reclamações de titulares de dados, discriminadas pelo tipo de obrigação, em face às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais e a quantidade de processos sancionatórios instaurados contra eles. Uma vez que não existem dados históricos sobre essas informações, a coleta e o acompanhamento desses dados poderão servir de base para eventuais revisões da alternativa escolhida.

3.3 TEMA 3 - SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO DE DADOS PESSOAIS E BOAS PRÁTICAS

3.3.1 RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

3.3.1.1 Introdução

A LGPD estabeleceu obrigações relacionadas à segurança e ao sigilo de dados, conforme disposto nos arts. 46, 47, 48 e 49, nos seguintes termos:

> *CAPÍTULO VII*
> *DA SEGURANÇA E DAS BOAS PRÁTICAS*
> ***Seção I***
> ***Da Segurança e do 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 A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.*
> *§ 2º As medidas de que trata o caput deste artigo 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 garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.*
> *Art. 48. O controlador deverá comunicar à autoridade nacional 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 pela autoridade nacional, 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 de a comunicação não ter sido imediata; e*
> *VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*
> *§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais 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, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.*

De acordo com a Norma ABNT NBR ISO/IEC 27001[45], a segurança da informação pode ser definida como o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação.

Esse conjunto de ações impacta todo o ambiente institucional das empresas com o objetivo de prevenir, detectar e combater as ameaças digitais, ou seja, estão relacionadas às camadas de tecnologia, processos e pessoas e não somente ao ambiente de tecnologia da informação.

Um importante ponto é o gerenciamento de riscos, que consiste no processo de identificar, quantificar e gerenciar os riscos relacionados à segurança da informação dentro da organização. Ele visa a obter um equilíbrio eficiente entre a concretização de oportunidades de ganhos e a minimização de vulnerabilidades e perdas.

Nesse sentido, existem diversos padrões recomendáveis, como por exemplo guias e frameworks, para operacionalizar a implementação de mecanismos relacionados à segurança da

[45] Norma ABNT NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. 2006.

informação. Cabe destacar que muitos mecanismos estão disponíveis gratuitamente, enquanto outros são utilizados como base para a certificação de conhecimentos profissionais.

Quanto às boas práticas e governança de dados, os arts. 50 e 51 da LGPD buscam estimular a sua adoção pelos controladores e operadores, nos seguintes termos:

> ***Seção II***
> ***Das Boas Práticas e da Governança***
> *Art. 50. Os controladores 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 controlador 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 do titular.*
> *§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:*
> *I - implementar programa de governança em privacidade que, no mínimo:*
> *a) demonstre o comprometimento do controlador 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 como se realizou sua coleta;*
> *c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;*
> *d) estabeleça políticas e salvaguardas adequadas com base em 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 a 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 da autoridade nacional ou de outra entidade responsável por promover o cumprimento de 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 pela autoridade nacional.*
> *Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.*

Segundo o *Data Governance Institute*, fórum internacional que publica frameworks, boas práticas e guias sobre o assunto, a governança de dados consiste em um procedimento de tomada de decisões e responsabilidades para com os processos relacionados aos dados.[46]

A governança de dados é importante mecanismo de controle e gerenciamento de dados, como por exemplo, qualidade de dados, arquitetura de dados, ciclo de vida de dados, dentre outros aspectos.

Nesse sentido, o conceito de governança de dados trazido pela LGPD é um tema bastante complexo e envolve atividades em diversas camadas, como aquelas relacionadas à cultura institucional, aos processos e à tecnologia da informação, não sendo, portanto, aplicável à maioria das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Para corroborar com essa evidência, cabe mencionar que um artigo da Harvard Business Review[47] de 2017 apontou que apenas 3% das empresas entrevistadas atingiram níveis de qualidade satisfatórios na governança que realizavam sobre seus dados.

Ainda, cabe salientar que, conforme o disposto no art. 50 da LGPD, não existe uma obrigação de implementação de regras de boas práticas e governança de dados para os controladores e os operadores. Entretanto, o §1º do art. 50 dispõe que, ao estabelecer as regras de boas práticas, o controlador 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 do titular.

Dessa forma, a lei estabeleceu possibilidade de uso de boas práticas internacionais, como por exemplo, a adoção de frameworks, para operacionalizar a governança de dados.

---

[46] *Data Governance Institute*. Disponível em: https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/. Acesso em 03/08/2021.
[47] Only 3% of Companies' Data Meets Basic Quality Standards. Disponível em: https://hbr.org/2017/09/only-3-of-companies-data-meets-basic-quality-standards. Acesso em: 03/08/2021.

3.3.1.2 Quais os problemas a serem solucionados?

Diversas contribuições recebidas durante a Tomada de Subsídios nº 1/2021 apontaram para a dificuldade de conformidade das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais com relação às obrigações ligadas à segurança e à governança de dados estabelecidas pela LGDP.

Conforme apresentado, a complexidade e o estado da arte relacionado ao tema segurança e governança de dados podem aumentar a não conformidade com a lei por microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais devido à falta de recursos financeiros e humanos, fato que pode expor os titulares a elevado risco de violação de seus dados pessoais.

Ademais, conforme já exposto, é importante considerar a baixa maturidade das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais com relação à proteção de dados e, para alterar esse cenário, faz-se importante buscar mecanismos regulatórios e institucionais para incentivar o amadurecimento do tema nesse grupo de agentes de tratamento.

Esse cenário deve ser considerado pela ANPD para a proposição do modelo regulatório capaz de induzir as microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais a proporcionar um ambiente mais seguro com relação aos dados dos titulares. Assim, o principal problema a ser solucionado é o risco de violação dos dados pessoais no tratamento de dados por microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais em razão da eventual não adoção de melhores práticas relacionadas à segurança da informação.

Outro problema identificado consiste nos custos de implantação de medidas de segurança da informação e boas prática, que, por serem altos, podem gerar dificuldade financeira às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, conforme já apontado neste relatório.

3.3.1.3 A Autoridade tem competência para atuar sobre os problemas?

Nos termos do que dispõe o art. 55-J, XVIII da LGPD, a ANPD tem competência para editar normas específicas, com procedimentos simplificados e diferenciados, bem como critérios de

elegibilidade, para que microempresas e empresas de pequeno porte, assim como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, possam adequar-se à LGPD.

3.3.1.4 Existe experiência internacional?

Sobre as experiências internacionais, destaca-se que autoridades de proteção de dados em todo o mundo atuam com abordagem orientativa e educativa, emitindo orientações e fornecendo ferramentas em apoio às pequenas e médias empresas para que busquem estar em conformidade com leis de privacidade e proteção de dados pessoais no que tange à segurança e boas práticas.

A título exemplificativo, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) publicou um guia para as pequenas e médias empresas sobre a segurança da informação.[48]

Outro ponto que deve ser destacado são as recomendações internacionais para apoiar a operacionalização da segurança da informação e a governança de dados nas organizações empresariais, que podem vir a subsidiar a elaboração de normas e guias sobre boas práticas a respeito do tema pela ANPD. Dentre essas recomendações, podem-se destacar:

(i) *Information Technology Infrasructure Library* – (ITIL): conjunto de regras que define as boas práticas de gestão de serviços de TI;

(ii) *Control Objectives for Information and Related Technologies (COBIT*)[49] – framework evolutivo de boas práticas de segurança, gestão e governança de TIC criado pela *Information Systems Audit and Control Association* (ISACA);

(iii) *Data Management Body of Knowledge*[50] *(*DAMA-DMBOK*)* – framework para a gestão e governança de dados;

(iv) Norma ABNT NBR ISO/IEC 20000 – trata da gestão da qualidade de serviços de tecnologia da informação e comunicação;

---

[48] ENISA. Guidelines for SMEs on the security of personal data processing, 2016. Disponível em https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. Acesso em 05/08/2021

[49] COBIT (*Control Objectives for Information and Related Technologies*). Disponível em: https://www.isaca.org/resources/cobit. Acesso em 04/08/2021.

[50] DMBOK (DAMA-DMBOK) *Data Management of Knowledge*. Disponível em: https://www.dama.org/cpages/body-of-knowledge. Acesso em 04/08/2021.

(v) Norma ABNT NBR ISO/IEC série 31000 – trata da avaliação e gestão de riscos;

(vi) Norma ABNT NBR ISO/IEC série 27000 – trata da segurança da informação;

(vii) *Secure Controls Framework*[51] (SCF) – catálogo de controles que trata de privacidade e segurança.

Essas recomendações internacionais são adotadas por grandes organizações empresariais no Brasil com vistas a operacionalizar as boas práticas com relação à segurança da informação e à governança de dados. No entanto, cabe lembrar que essas recomendações são elaboradas considerando o estado da arte sobre a gestão de tecnologia da informação e a governança de dados, e demandam maturidade institucional em relação ao tema.

3.3.1.5 Quais os objetivos da ação? Por que a intervenção regulatória é necessária?

O objetivo imediato da intervenção, conforme mencionado ao longo do presente relatório de AIR, é atender ao comando do art. 55-J, XVIII da LGPD e editar norma específica para simplificar e diferenciar os procedimentos para que microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam se adequar à referida lei.

Por sua vez, o objetivo mediato consiste em facilitar a adaptação desse grupo à LGPD, promovendo a sua conformidade e contribuindo para a disseminação da cultura de proteção de dados pessoais.

Especificamente no que se refere à segurança da informação, pretende-se conscientizar as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais da sua importância e dos riscos e danos a que se expõem ao não adotarem as medidas necessárias. Além disso, ao conscientizar esse grupo de agentes de tratamento, espera-se aumentar a segurança do tratamento dos dados pessoais, beneficiando, assim, os titulares de dados pessoais.

3.3.1.6 Quais os grupos afetados?

A norma de aplicação da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais impacta todos os titulares de dados que se relacionam com esses agentes de tratamento. Diante disso, ao proceder o levantamento dos agentes

[51] SCF - *Secure Controls Framework*. Disponível em: https://www.securecontrolsframework.com/. Acesso em: 04/08/2021.

econômicos, dos usuários dos serviços prestados e dos demais afetados pelo problema ora analisado, os grupos a seguir foram identificados como mais impactados:

i) agentes de tratamento de dados, em especial aqueles em que se enquadram as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais;

ii) titulares de dados pessoais;

iii) fabricantes de *softwares* de gestão e governança de dados;

iv) prestadores de serviço de consultoria;

v) encarregados.

Outros grupos identificados, como órgãos de pesquisa, órgãos públicos, agências reguladoras e imprensa poderão ser afetados, mas com impactos reduzidos ou na medida em que se relacionarem com microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

3.3.2. ANÁLISE DAS ALTERNATIVAS

3.3.2.1 Quais são as opções regulatórias consideradas para o tema?

Em relação ao tema segurança da informação e sua aplicação às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, foram identificadas duas opções para endereçamento do tema.

A primeira opção consistiria em incluir na norma a ser editada uma lista de ações e obrigações mínimas que esse grupo de agentes de tratamento deverá seguir para conferir segurança ao seu tratamento de dados pessoais. Se por um lado a inclusão em norma promoveria maior segurança jurídica e, em razão da natureza da norma, poderia garantir aos titulares de dados uma confiança maior em relação ao tratamento de dados pessoais, a definição de normas dessa natureza para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais sem o estabelecimento de normas gerais para todos os agentes de tratamento significaria, na prática, um ônus a esse grupo específico de agentes de tratamento.

Além disso, essa opção implicaria aumentar os custos de adaptação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais à LGPD; tendo

em vista que as empresas não costumam investir em mecanismos relacionados à segurança da informação, essa adaptação muito provavelmente seria totalmente nova para essas empresas.

Outra opção consistiria em uma intervenção não regulatória, que perpassaria pela atividade orientadora da ANPD, assunto levantado como uma atuação esperada pelas empresas em diversas contribuições recebidas no âmbito da Tomada de Subsídios nº 01/2021. No caso, seria possível a edição de um guia orientativo, com as sugestões de ações que podem ser tomadas pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais e com orientações sobre o porquê elas são importantes e quais são os benefícios de sua adoção.

Essa ação disseminaria o conhecimento sobre o assunto de forma mais completa e com uma linguagem mais simples do que uma norma, e, ao mesmo tempo, não criaria obrigações para as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. Além disso, ao trabalhar no âmbito da orientação e conscientização, a ação tenderia a proteger também os direitos dos titulares de dados.

Além disso, salienta-se que independentemente da adoção de uma das alternativas regulatórias propostas, entende-se cabível que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam estabelecer uma política de segurança da informação (PSI) simplificada.

A PSI consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.

Deve-se reconhecer que a elaboração da PSI não é uma obrigação expressamente disposta na LGPD, mas vale ressaltar que a PSI, tendo como base as recomendações internacionais, faz parte das medidas administrativas citadas no art. 46 da LGPD.

Essa política pode ser elaborada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança da informação. Entretanto, a PSI tende a ser mais aplicável às organizações de médio e grande porte, que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Entende-se, assim, que cabe a cada instituição avaliar os impactos e os recursos necessários para sua implementação, para então decidirem sobre

a sua formalização, sendo que esta Autoridade estimula a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

Diante disso, infere-se ser adequado incluir na minuta da resolução uma possível política simplificada de segurança da informação, levando em consideração o nível de risco do tratamento de dados para os direitos e liberdades do titular, bem como os custos relacionados à sua aplicação, à realidade financeira dos agentes e à disponibilidade de recursos, inclusive os financeiros e de pessoal especializado na organização.

3.3.2.2 Alternativa A - Adoção de modelo regulatório com disposição das obrigações relacionadas à segurança da informação em resolução

A alternativa A baseia-se na abordagem regulatória de publicação de um normativo com a definição de requisitos mínimos para garantir a segurança da informação no tratamento de dados por microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais.

Conforme já citado, esse modelo, em tese, pode garantir maior segurança no tratamento de dados pessoais, mas demandaria vultuosos investimento de recursos financeiros e humanos para atender a conformidade, podendo impactar sobremaneira a operação desses agentes. Além disso, a edição de norma não atingiria o propósito de orientar esse grupo de agentes sobre a matéria.

Resumo da análise da alternativa A

Grupos afetados	Desafios	Benefícios
ANPD	Necessidade de monitoramento específico de obrigações para agentes que ainda não foram definidos como microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais. Sem possibilidade de atuação orientadora. Sem possibilidade de aprofundamento do tema no texto normativo.	Não foram identificados benefícios relevantes.
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Dificuldade de se ajustar às obrigações. Criação de disparidade de obrigações em razão da inexistência de obrigações nesse sentido para os demais agentes de tratamento.	Maior segurança jurídica quanto ao que se espera.

Titulares de dados pessoais	Não foram identificados desafios relevantes.	Sensação inicial de maior confiança em relação ao tratamento e segurança da informação desse grupo de agentes de tratamento.
Fabricantes de *softwares* de gestão e governança de dados	Necessidade de adaptação ao novo modelo.	Previsibilidade das ações da ANPD.
Prestadores de serviço de consultoria	Necessidade de adaptação ao novo modelo.	Previsibilidade das ações da ANPD.
Encarregados	Necessidade de adaptação ao novo modelo regulatório.	Previsibilidade das ações da ANPD.

3.3.2.3 Alternativa B - Adoção de modelo regulatório baseado em guia de orientação de boas práticas relacionado à segurança da informação

A alternativa B fundamenta-se na abordagem orientativa e educativa com a publicação, principalmente, de guias de boas práticas. Essa proposta está em linha com o art. 55-J, XVIII, que concedeu à ANPD a competência para editar orientações para que microempresas, empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação possam adequar-se à LGPD.

Como já citado, essa alternativa disseminaria o conhecimento sobre o assunto de forma mais completa e com uma linguagem mais acessível do que a de uma norma, e, ao mesmo tempo, não criaria obrigações específicas para esse grupo de agentes sem a definição de normas gerais para os demais. Além disso, essa opção, em tese, protege também os direitos dos titulares de dados, que tenderiam a ter confiança no que se refere à segurança no tratamento dos seus dados.

Resumo da análise da alternativa B

Grupos afetados	Desafios	Benefícios
ANPD	Atualização periódica do guia orientativo a partir das sugestões e dúvidas enviadas.	Diminuição das atividades a serem realizadas no âmbito da fiscalização, tendo em vista se tratar de uma atividade orientadora. Possibilidade de aprofundar e educar esse grupo de agentes de tratamento sobre o assunto.
Microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais	Necessidade de estudo e de adaptação gradual ao que o guia estabelecer como boas práticas.	Menor custo regulatório de adaptação. Possibilidade de adequação efetiva e gradual ao que se espera como boas-práticas de segurança da informação.

Titulares de dados pessoais	Sensação inicial de inexistência de proteção ou obrigações referentes à segurança da informação.	Ao médio e longo prazo, maior segurança no tratamento dos dados pessoais.
Fabricantes de *softwares* de gestão e governança de dados	Necessidade de estudo do que a ANPD considera como essencial para empresas.	Possibilidade de adaptação gradual ao que a ANPD espera.
Prestadores de serviço de consultoria	Necessidade de estudo do que a ANPD considera como essencial para empresas.	Possibilidade de adaptação gradual ao que a ANPD espera.
Encarregados	Necessidade de adaptação ao novo modelo.	Possibilidade de adaptação gradual ao que a ANPD espera.

3.3.3 CONCLUSÃO E ALTERNATIVA SUGERIDA

3.3.3.1 Qual a conclusão da análise realizada?

Considerando as alternativas apresentadas como solução para os problemas relacionados à segurança da informação, identificou-se que, em razão dos desafios e benefícios elencados para cada um dos grupos afetados, que a **Alternativa B** é a mais adequada para endereçar o tema.

Essa conclusão decorre da possibilidade de atuação no âmbito da atividade de orientação da ANPD que o guia orientativo possibilita, tendo em vista que é possível tratar o tema da segurança da informação de forma mais expressiva, ou seja, com maior profundidade, e educativa em um instrumento dessa natureza.

3.3.3.2 Como será operacionalizada a alternativa sugerida?

Com relação ao tema de segurança da informação e boas práticas, entende-se que criar instrumentos capazes de potencializar a sua operacionalização pelas microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, como por exemplo, guias de boas práticas e procedimentos simplificados, é o mais adequado.

Para isso, será necessário que a ANPD realize um levantamento dos padrões e guias que possam apoiar a operacionalização da segurança da informação nas organizações empresariais e possam subsidiar a elaboração de boas práticas pela ANPD, podendo-se destacar ao menos as normas da *International Organization for Standardization* (ISO), organização internacional que desenvolve e publica normas técnicas que são utilizadas por muitos países, incluindo o Brasil. No

caso, cabe dar destaque para a Norma ABNT NBR ISO/IEC 27001[52], que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.

Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam a gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, essa norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação dentro do contexto dos riscos de negócio globais de uma organização.

Após o estudo do material disponível, será necessário que a ANPD elabore um guia orientativo sobre a matéria e o disponibilize com a brevidade que o tema requer. Por se tratar de um guia orientativo, é importante que o material deixe claro que as ações ali elencadas são sugestões para esse grupo de agentes de tratamento.

3.3.3.3 Como a alternativa sugerida será monitorada?

Um guia orientativo de boas práticas não é de observância obrigatória, mas tão somente busca orientar e apoiar a adequação das microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais em relação à LGPD. Ainda assim, será possível acompanhar se as orientações e indicações da ANPD sobre a segurança da informação estão sendo seguidas por meio do acompanhamento das atividades de fiscalização da Coordenação-Geral de Fiscalização, bem como por meio de elaboração dos relatórios anuais de gestão da ANPD. No caso, será possível aferir se as reclamações sobre esses agentes de tratamento advêm da não atenção de boas práticas sobre segurança.

Nesse sentido, sugere-se acompanhar a quantidade de reclamações de titulares de dados em face a esses agentes e a quantidade de processos sancionatórios instaurados contra eles. Uma vez que não existem dados históricos sobre essas informações, a coleta e o acompanhamento desses dados poderão servir de base para eventuais revisões da alternativa escolhida.

Outra forma de monitorar a efetividade das orientações sobre segurança e boas práticas consiste no acompanhamento da quantidade de notificações de incidentes de segurança por

[52] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais recebidas pela ANPD.

4. CONCLUSÃO

O presente relatório de AIR apresenta os pontos que foram estudados pela ANPD para elaboração da minuta de resolução sobre a aplicação da LGPD para microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, tendo sido feita uma divisão em 3 (três) grandes temas: (i) a definição do grupo de agentes aos quais a norma a ser editada se destinará; (ii) conformidade em relação às obrigações da LGPD; e (iii) segurança da informação.

Com relação ao tema 1, optou-se pela **alternativa B** por entender que a melhor opção para se definir os destinatários da norma a ser editada consiste em considerar os critérios adequados que permitam a simplificação e flexibilização de determinada obrigação sem aumentar consideravelmente os riscos envolvidos, tanto para os titulares de dados quanto para esse grupo de agentes de tratamento.

Assim, concluiu-se que a melhor forma de atingir esse critério é por meio da criação de um conceito base que inclua as microempresas, empresas de pequeno porte e *startups*, com os demais critérios identificados ao longo do processo de coleta de informações.

Nesse sentido, revelam-se como apropriados adotar como conceitos-base os trazidos pela Lei Complementar nº 123/2006 para as microempresas, empresas de pequeno porte e *startups*. Além disso, para as *startups*, cabe também adotar os parâmetros trazidos pela Lei Complementar nº 182/2021, conforme o seu art. 4º, inclusive para fins de faturamento máximo para todos os agentes de tratamento os quais a resolução se destina.

Esses conceitos serão considerados em conjunto com outros critérios especificados ao longo do regulamento, tendo em vista que entidades que não se enquadram nos conceitos mencionados mas que, ao se pensar na lógica do que se pretende com essa norma de aplicação da LGPD, podem ser equiparadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, quais sejam, as pessoas jurídicas sem fins lucrativos, como associações, fundações, organizações religiosas e partidos políticos.

Entende-se que esse grupo de agentes de tratamento deve ter uma denominação específica a ser apresentada na norma a ser editada, sugerindo-se, aqui, a adoção do termo agentes de tratamento de pequeno porte.

Concluiu-se, ainda, pela adoção de uma classificação do tratamento realizado em razão do risco que ele implica aos titulares de dados, tendo em vista ser mais efetivo na proteção dos direitos dos titulares de dados, ao mesmo tempo que gera menos insegurança para fins do trabalho de fiscalização da ANPD.

Por sua vez, em relação ao tema 2 concluiu-se que a opção mais adequada é a **alternativa A**, que consiste na edição de um normativo único para apresentar o tratamento diferenciado das obrigações disposta na LGPD para que as microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais possam se adequar à lei.

Na análise foi considerada a divisão das obrigações dispostas na LGPD da seguinte forma: i) obrigações relacionadas aos direitos do titular; ii) registro das atividades de tratamento, iii) relatório de impacto à proteção de dados pessoais; iv) comunicação de incidentes de segurança; v) encarregado; e vi) prazos diferenciados.

Cabe esclarecer que se concluiu pela norma única que contenha a definição do conceito do grupo de agentes de tratamento aos quais a norma se aplicará e os critérios para sua incidência, bem como a definição do regime diferenciado em relação a algumas obrigações identificadas como passíveis de flexibilização no presente momento para as microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, sem que isso prejudique os direitos dos titulares de dados.

Ao mesmo tempo, tendo em vista ser necessário reconhecer que as flexibilizações relacionadas às obrigações mais complexas precisam de análise mais profunda, sugeriu-se também que elas deverão ocorrer, portanto, no âmbito dos projetos de elaboração das resoluções específicas.

Já em relação ao tema 3, concluiu-se que a sugestão mais adequada baseia-se na **alternativa B**, com a edição de um guia orientativo sobre segurança da informação voltado às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais, tendo em vista que esse instrumento disseminará o conhecimento sobre o assunto de forma mais completa e com

uma linguagem mais acessível do que a de uma norma, e, ao mesmo tempo, não criaria obrigações específicas para esse grupo de agentes de tratamento sem a definição de normas gerais para os demais.

Além disso, essa opção protege também os direitos dos titulares de dados, que tenderiam a ter confiança no que se refere à segurança no tratamento dos seus dados.