PAÍS DA AUTORIDADE	OBJETO	VALOR DA MULTA
 Dinamarca	Ausência de delimitação dos prazos de retenção e descarte dos dados pessoais de clientes por empresa de design. Resumo da decisão **aqui**.	200.800€(duzentos mil e oitocentos euros)
 França	Excesso de monitoramento por câmeras de segurança por uma microempresa (de nove funcionários), além de medidas de segurança insuficientes, mesmo após notificação prévia da CNIL. Decisão **aqui.**	20.000€ (vinte mil euros)
 Noruega	Distribuição ilegal (ausência de base legal) de uma gravação do sistema de monitoramento de uma loja. Resumo da decisão **aqui**.	40.000€ (quarenta mil euros)

PAÍS DA AUTORIDADE	OBJETO	VALOR DA MULTA
 Reino Unido	Venda dos dados pessoais dos usuários do site sem o seu consentimento, após oferecer conselhos gratuitos sobre o período da gravidez e maternidade. Decisão **aqui**.	140.000£ (cento e quarenta mil libras)
	Envio de milhões de mensagens de marketing não solicitadas. Multa aplicada após a reclamação de cerca de 2.100 pessoas. Decisão **aqui**.	200.000£ (duzentos mil libras)
	Realização de 1.6 milhões de ligações não solicitadas para os assinantes de uma empresa de design de quartos. Decisão **aqui**.	160.000£ (cento e sessenta mil libras)
	Realização de 213 ligações não solicitadas por escritório de advocacia inglês. Decisão **aqui**.	80.000£ (oitenta mil libras)

A REGULAÇÃO DO TRATAMENTO DE DADOS POR AGENTES DE PEQUENO PORTE PELO GDPR

- O **Art.30 (5)**, do Regulamento de Proteção de Dados Europeu (GDPR) dispensa as micro, pequenas e médias empresas com menos de 250 empregados da obrigação de manter os registros das atividades de tratamento de dados pessoais, seja na qualidade de controlador ou operador[24].
- Essa exceção não se aplica se o processamento de dados:

01. trouxer riscos aos direitos e liberdade dos titulares;
02. ocorrer regularmente; ou
03. abranger as categorias especiais de dados a que se refere o **Artigo 9(1)**, ou dados pessoais relativos a condenações penais e infrações referidos no **Artigo 10**.

[24]. Disponível em: **https://gdpr-info.eu/recitals/no-13/**. Acessado em 09.02.2021. **(13)** To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC ([5])

ORIENTAÇÃO

- Em âmbito nacional, as autoridades de proteção de dados europeias adotaram diversas medidas para auxiliar a implementação do GDPR em micro, pequenas e médias empresas, como pode ser visto na seção a seguir.

MULTAS

- Quanto às multas aplicadas, após a análise do quadro apresentado no ponto "*Multas por violação à proteção de dados praticada por empresas de pequeno e médio porte*" disponível no material de apoio, é possível ter uma melhor noção da faixa de valor de multa aplicada nesses casos.

  Observamos que, antes da aplicação de fato da multa, diversas autoridades alertaram os agentes de pequeno porte acerca da violação ao GDPR na forma de um aviso prévio em conjunto com uma requisição para corrigir tal violação.

  Caso essa requisição não fosse atendida pelo agente, a multa era devidamente aplicada. É o que ocorreu no caso da multa de vinte e mil euros aplicada pela Autoridade de Proteção de Dados francesa (CNIL) a uma microempresa de tradução por excesso de monitoramento de seus funcionários[25].

[25] Videosurveillance: CNIL issues fine of 20,000 euros against a small company in France. Disponível em: <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/videosurveillance-cnil-issues-fine-of-20-000-euros-against-a-small-company-in-france>.

O PROGRAMA DE GOVERNANÇA DE DADOS PESSOAIS

- Segundo o Instituto Brasileiro de Governança Corporativa (IBGC), o termo governança corporativa pode ser resumido como o sistema de gestão e monitoramento que envolve todos os níveis de uma organização, através do qual seus princípios e valores básicos são convertidos em recomendações objetivas, de modo a alinhar seu interesse com a finalidade de preservá-la e otimizar o seu valor econômico de longo prazo.

- A Governança de Dados Pessoais, portanto, refere-se à observância das obrigações estabelecidas pela LGPD no desenvolvimento do sistema de gestão de uma organização para que as suas atividades estejam em conformidade com a legislação.

ETAPAS PARA IMPLEMENTAÇÃO DO PROGRAMA DE GOVERNANÇA DE PROTEÇÃO DE DADOS

- Diante da complexidade e multidisciplinaridade das ações necessárias para implementação do programa de governança de proteção de dados, recomendamos a utilização da metodologia e ferramentas de modelagem de processos de negócio.

  O ciclo de vida do projeto de modelagem de processos aplicado ao programa de governança de proteção de dados, possui cinco etapas:

01. planejamento;
02. execução do projeto;
03. análise de melhorias e redesenho de processos;
04. implantação;
05. monitoramento e controle das mudanças necessárias para adequação das atividades das organizações à LGPD.

PLANEJAMENTO

- Definição da estratégia de governança: caracterização da organização e do tipo de negócio, identificação e priorização dos processos críticos quanto ao tratamento de dados pessoais, definição de metas e objetivos.

MAPEAMENTO

- Mapeamento de atividades de tratamento de dados através de ferramentas de levantamento de informações com os agentes que participam das atividades de tratamento de dados (da aplicação de questionários, entrevistas, realização de workshops, entre outros).

REDESENHO

- Atribuição das bases legais adotadas para o tratamento de dados pessoais.
- Elaboração de medidas de regularização das atividades de tratamento de dados pessoais (elaboração de relatórios de impacto à proteção de dados pessoais, gestão do consentimento dos titulares de dados pessoais).
- Comparação das rotinas de tratamento de dados adotadas com as disposições legais, normas técnicas e melhores práticas do mercado, sugestões de medidas de correção e melhoria de atividades de tratamento de dados.

IMPLEMENTAÇÃO

- Divulgação dos novos processos, orientação dos agentes de tratamento de dados pessoais, através da elaboração de material didático para os agentes de tratamento de dados, estabelecimento de canal para exercício de direitos dos titulares de dados pessoais.

MONITORAMENTO E CONTROLE

- Revisão periódica do mapeamento de atividades de tratamento de dados pessoais, resposta a questionamentos internos e desenvolvimento de atividades de tratamento de dados por protocolos de *privacy by design*, suporte aos titulares de dados para o exercício de seus direitos, verificação da continuidade do programa de governança e, caso necessário, o redesenho de soluções para atendimento das demandas da organização quanto a privacidade e proteção de dados.

OBRIGAÇÕES DOS AGENTES DE TRATAMENTO SEGUNDO À LGPD E OS IMPACTOS AOS AGENTES DE PEQUENO PORTE

> "A lei impõe aos agentes de tratamento de 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, bem como garantia de segurança, boas práticas e governança de dados pessoais." [26]

[26] Parágrafo 13. Nota Técnica nº 1/2021/CGN/ANPD. Coordenação-Geral de Normatização. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica.pdf. Acesso em 18.02.2021

O quadro a seguir descreve as obrigações impostas aos agentes de tratamento de dados pessoais pela LGPD e os documentos gerados durante o programa de proteção de dados. **Destacam-se os impactos para a instrumentalização dos mesmos:**

01. Dispor de recursos financeiros para a execução e/ou terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais;

02. Possuir conhecimento jurídico, além de técnico nas áreas de: mapeamento de processos e segurança da informação.

03. Dispor de tempo hábil disponível para se desenvolver o projeto e construir cultura interna de proteção de dados.

DOCUMENTO/OBRIGAÇÃO	O QUE É
Registro das operações de tratamento de dados pessoais	Lista todas as atividades de tratamento de dados realizadas pela empresa. Obrigação legal estabelecida pela LGPD (art. 37) para todas as empresas
Relatório de impacto à proteção de dados pessoais	Contém a descrição das operações de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Seu objetivo é apontar medidas, salvaguardas e mecanismos de mitigação desses riscos. Obrigação legal estabelecida pela LGPD (art. 10 § 3°, art. 38).

DOCUMENTO/OBRIGAÇÃO	O QUE É
Gestão do Consentimento	Procedimentos que possibilitam que o titular de dados pessoais ou seu responsável manifeste sua vontade em consentir com a realização de procedimento com finalidade específica, assegurando-lhe o direito de decisão quanto ao tratamento proposto pelo controlador. Indicado para a realização de tratamento de dados de menores de idade (art. 14) ou quando a base legal para o tratamento de dados pessoais do titular for baseada no consentimento (art. 8°).
Programa de Segurança da Informação	**i ABNT NBR ISO/IEC 27001** Tecnologia da informação Técnicas de segurança Requisitos Sistemas de gestão da segurança da informação **ii ABNT NBR ISO/IEC 27002** Tecnologia da informação Técnicas de segurança Código de prática para controles de segurança da informação. Demonstra os riscos e vulnerabilidades dos dados tratados pela empresa bem como medidas de mitigação e segurança aplicáveis às rotinas das empresas através de projeto de segurança da informação.

DOCUMENTO/OBRIGAÇÃO	O QUE É
Programa de Gestão de Riscos	O programa de avaliação de riscos tem como referência a norma **ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes**, e assim como o programa de segurança da informação, para a efetividade da gestão de risco é necessária a elaboração do programa de gestão de risco, onde é realizado o levantamento dos ativos de dados da organização, a análise de riscos e vulnerabilidades aos quais estão expostos, os critérios de aceitação de risco, as medidas de mitigação, os controles e documentação e os procedimentos de acompanhamento e melhoria do projeto.
Políticas de Privacidade e Proteção de Dados	Demonstra, de modo transparente, de que forma a organização realiza o tratamento de dados pessoais de titulares de dados.
Garantia de segurança, boas práticas e governança de dados pessoais	Orientação de todos os agentes envolvidos no tratamento de dados pessoais, internos ou externos à organização. Pode ser realizado através do estabelecimento de Política de Fornecedores, Guias de Compliance, entre outros.

SANDBOX REGULATÓRIO

- Objeto: Desenvolvimento de sites e/ou aplicativos inovadores para instrumentalização do cumprimento das obrigações legais estabelecidas na Lei Geral de Proteção de Dados e das atribuições delegadas a Autoridade Nacional de Proteção de Dados pelo Decreto .

PORTAL EMPREENDEDOR

- Atualmente o **Portal do Empreendedor** reúne um conjunto de soluções e conteúdo para microempreendedores individuais (MEI). Para facilitar o acesso à informação e a efetividade das proposições que se aplicam a rotina do MEI, sugerimos:.

01. Incorporação das disposições da Lei Geral de Proteção de Dados, de forma simplificada na seção Direitos e Deveres
02. Desenvolvimento de curso básico de Boas Práticas em Proteção de Dados, com emissão de certificado/declaração
03. Aplicação de questionários periódicos para compreensão das rotinas de tratamento de dados desenvolvidas por MEIs
04. Automatização de emissão de Registro de Operações de Tratamento de Dados Pessoais, como serviço oferecido através do Portal do Empreendedor
05. Automatização de emissão de Relatório de Impacto ao Tratamento de Dados Pessoais, em conjunto com Guia de Boas Práticas em Proteção de Dados

06. Canal para tirar dúvidas frequentes para titulares e MEIs

07. Canal para exercício de direitos de titulares incorporada ao Portal

08. Canal para denúncias, advertências, multas e procedimento administrativo

SITE AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

01. Aplicação de questionários periódicos para compreensão das rotinas de tratamento de dados por agentes de tratamento

02. Canal de Autoavaliação da organização

03. Automatização de emissão de Registro de Operações de Tratamento de Dados Pessoais

04. Automatização de emissão de Relatório de Impacto ao Tratamento de Dados Pessoais

05. Canal para exercício de direitos de titulares incorporada ao Portal

06. Canal para denúncias, advertências, multas e procedimento administrativo

LIMA FEIGELSON

ADVOGADOS

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: LIMA FEIGELSON ADVOGADOS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável a microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e o mapeamento de experiências internacionais que tratem do tema; e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quais são os desafios/problemas regulatórios relacionados ao tema?	Os obstáculos competitivos se materializam na disponibilidade limitada de recursos que microempresas, empresas de pequeno porte, *startups* e MEIs que tratam dados pessoais com fins econômicos podem destinar à adequação às exigências estabelecidas pela Lei Geral de Proteção de Dados. De modo geral, empresas menores são compostas por equipes menos diversificadas e com menor grau de especialização, logo, a falta de conhecimento e informação acerca da legislação somada ao nível de complexidade de um projeto de *adequação* à LGPD agravam as dificuldades enfrentadas por pequenas empresas.[1]

[1] HARTMAN, Dex. **GDPR in Small Business: The Antecedents of Compliance.** Dissertação de Mestrado. University of Groningen (Países Baixos). Disponível em: <https://feb.studenttheses.ub.rug.nl/22668/1/Master_Thesis_SBE.pdf>. Acesso em: 09.02.2021

	As disposições de proteção de dados irão acrescer ainda mais obrigações em termos de normas e regulamentos que incidem sobre os mais de 9 (nove) milhões de empreendedores individuais e as quase 7,5 (sete vírgula cinco) milhões de pequenas empresas do Brasil[2]. Portanto, os desafios da ANPD estão atrelados aos custos e riscos que as exigências legais trazem à manutenção das atividades empresariais, de maneira que se evite o déficit competitivo dos agentes de pequeno porte face à estrutura mais desenvolvida de que gozam as grandes empresas.
Existem sugestões para endereçamento do problema?	Nossas sugestões estão disponíveis no Material de Apoio a Tomada De Subsídios Nº 1 /2021, e podem ser consultadas nas páginas 5 a 15. Em resumo, se relacionam com os seguintes tópicos: 1. Categorização dos agentes de tratamento para atribuição e dispensa de obrigações legais; 2. Criação de canal institucional que atenda a demanda de empresas e Titulares de Dados; 3. Indicação de critérios para aplicação de multas.
Quais são as oportunidades relacionadas ao tema?	Expressar em marco regulatório o incentivo à construção da cultura de proteção de dados, através da orientação e suporte aos micro e pequenos empresários, onerando-os o mínimo possível e gerando autonomia para que possam construir oportunidades de negócio de forma segura.
Quais são as experiências internacionais sobre o tema?	Considerando a importância econômica dos Agentes de Tratamento em empresas de pequeno porte e os desafios para implementação da cultura de proteção de dados, diversas iniciativas foram tomadas para auxiliar a adequação desses Agentes às leis de proteção de dados internacionais. Nossa pesquisa contemplou as ações desenvolvidas por 11 (onze) países, para ter acesso ao

[2] SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). **Dados do Data Sebrae.** Disponível em: <https://datasebrae.com.br/totaldeempresas/>. Acesso em: 14.02.2021

	conteúdo completo, consulte o Material de Apoio a Tomada De Subsídios Nº 1 /2021, nas páginas 15 a 23.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Nossas sugestões estão disponíveis no Material de Apoio a Tomada De Subsídios Nº 1 /2021, e podem ser consultadas nas páginas 5 a 15. Em resumo, se relacionam com os seguintes tópicos: 1. Tipo de negócio (*Business to Business*, *Business to Consumers*, *Business to Business to Consumers*, *Business to Government* e outros; 2. Quantidade de funcionários, volume de faturamento do negócio e balanço total (critério financeiro); 3. Atividade desenvolvida da empresa.
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)?	As contribuições para essa seção podem ser consultadas nas páginas 24 e 25 do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Nossa pesquisa abordou os seguintes tópicos: 1. A Regulação do Tratamento de Dados por Agentes de Tratamento em empresas de pequeno porte pelo GDPR; 2. Orientação; 3. Multas.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	As contribuições para essa seção podem ser consultadas na página x do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Consideramos as etapas e técnicas sugeridas para construção efetiva do documento regulatório. Em síntese, destacam-se os seguintes impactos: 1. Alocar recursos de tempo para a execução e/ou financeiros para terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais;

	2. Possuir conhecimento nas áreas de: mapeamento de processos, segurança da informação e na área jurídica de privacidade e proteção de dados. 3. Dedicar tempo hábil para o desenvolvimento do projeto, investindo para a construção e manutenção da cultura interna de proteção de dados.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	De acordo com o art. 5º, VIII da LGPD, o Encarregado de Dados será indicado pelo Controlador e pelo Operador e atuará como canal de comunicação entre o agente de tratamento de dados, os Titulares e a Autoridade Nacional de Proteção de Dados. Ainda que a Autoridade Nacional de Proteção de Dados não tenha emitido diretrizes quanto às funções e às qualificações necessárias para o desenvolvimento das atividades de Encarregado de Dados, sabemos tal profissional deverá ser altamente qualificado. O Encarregado de Dados deve possuir conhecimento abrangente acerca dos processos da empresa, bem como da legislação brasileira, sobretudo, mas não se limitando à LGPD, Código Civil, Código de Defesa do Consumidor, Consolidação das Leis do Trabalho bem como das melhores práticas internacionais acerca de privacidade e proteção de dados e o domínio das ferramentas de gestão de processos. Assim, **a nomeação do Encarregado de Dados por Agentes de Tratamento em empresas de pequeno porte implicará em custos significativos, seja por capacitação, contratação direta ou terceirização**. Recomendamos que a nomeação de Encarregado de Dados para empresas de pequeno porte somente seja exigível nas hipóteses de organizações cuja atividade principal seja o tratamento de dados pessoais. Particularmente, para os microempreendedores individuais (MEI), entendemos que a nomeação de um Encarregado de Dados seja dispensável.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	As contribuições para essa seção podem ser consultadas nas páginas 26 a 31 do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Consideramos as etapas e técnicas sugeridas para construção efetiva do documento regulatório. Em síntese, destacam-se os seguintes impactos:

	1. Dispor de recursos financeiros para a capacitação, execução e/ou terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais; 2. Possuir conhecimento técnico nas áreas de: mapeamento de processos, segurança da informação, direito e *design;* 3. Dispor de tempo hábil disponível para se desenvolver o projeto e construir cultura interna de proteção de dados.
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?	**Dados Pessoais Sensíveis:** Previstos no art. 5º, II da LGPD, os dados pessoais sensíveis recebem um tratamento singular em razão de sua potencial utilização discriminatória ou lesiva, capaz de revelar aspectos íntimos ligados à personalidade humana[3]. Devido às suas características, a Lei estabelece que a ANPD poderá solicitar a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), além de sobre padrões técnicos mínimos para o tratamento de dados pessoais sensíveis. Assim, **as empresas de pequeno porte deverão arcar com os custos de elaboração de RIPD e adoção de medidas de segurança.** **Dados de Crianças e Adolescentes:** O ordenamento jurídico brasileiro conferiu à criança e ao adolescente tutela diferenciada, visando proteger seu desenvolvimento. A LGPD aponta para o mesmo sentido ao afirmar que o tratamento deverá ser realizado no melhor interesse da criança e do adolescente (art. 14, LGPD). Assim, exige-se a obtenção de consentimento específico e destacado de pelo menos um dos pais ou responsável legal. De acordo com a LGPD, o consentimento consiste na manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. No tocante ao tratamento de dados de crianças e adolescentes, inclui-se **o desafio da gestão do consentimento que envolve: (i) informar ao responsável pelo titular os aspectos**

[3] DONEDA, 2006, p. 160-161.

	relacionados ao tratamento; (ii) coletar e; (iii) armazenar adequadamente o manifestação do consentimento. A gestão do consentimento requer treinamento específico do Operador para que informe devidamente ao responsável sobre o tratamento de dados, além da instrumentalização da obtenção do consentimento, que deverá se dar mediante termo assinado.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	As contribuições para essa seção podem ser consultadas nas páginas 26 a 31 do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Consideramos as etapas e técnicas sugeridas para construção do programa de governança de dados. Em síntese, destacam-se os seguintes impactos: 1. Dispor de recursos financeiros para a capacitação de colaboradores, execução e/ou terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais; 2. Possuir conhecimento técnico nas áreas de: mapeamento de processos, segurança da informação, direito e *design;* 3. Dispor de tempo hábil disponível para se desenvolver o projeto e construir cultura interna de proteção de dados.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	As contribuições para essa seção podem ser consultadas nas páginas 26 a 31 do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Consideramos as etapas e técnicas sugeridas para construção efetiva do documento. Em síntese, destacam-se os seguintes impactos: 1. Dispor de recursos financeiros para a execução e/ou terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais; 2. Possuir conhecimento jurídico, além de técnico nas áreas de mapeamento de processos e segurança da informação.

	3. Dispor de tempo hábil disponível para se desenvolver o projeto e construir cultura interna de proteção de dados. Ressalte-se que a aplicação de padrões de segurança varia de acordo com a natureza dos serviços prestados, dos dados tratados e com a capacidade financeira do Agente de Tratamento de Dados. Assim, não será razoável exigir de Agentes de Tratamento em empresas de pequeno porte a adoção de padrões altamente rígidos e custosos, sob pena de impor-se obstáculo à manutenção da atividade empresarial, especialmente daqueles que não tratam dados pessoais sensíveis.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	As contribuições para essa seção podem ser consultadas nas páginas 26 a 31 do Material de Apoio a Tomada De Subsídios Nº 1 /2021. Consideramos as etapas e técnicas sugeridas para construção efetiva do documento. Em síntese, destacam-se os seguintes impactos: 1. Dispor de recursos financeiros para a capacitação, execução e/ou terceirização do projeto de governança de proteção de dados e instrumentalização das obrigações legais; 2. Possuir conhecimento jurídico, além de técnico nas áreas de mapeamento de processos, gestão contratual e segurança da informação. 3. Dispor de tempo hábil disponível para se desenvolver o projeto e construir cultura interna de proteção de dados.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Além do aspecto concorrencial, o direito à portabilidade busca engajar o Titular de Dados a fim de que ele possa dispor dos seus dados pessoais, constituindo um elemento fundamental para o exercício da autodeterminação informativa. Contudo, este direito apresenta 3 (três) principais desafios que tornam a implantação da portabilidade ainda mais complexam para as empresas de pequeno porte. Em primeiro lugar, cumpre destacar que ainda não há regulamentação que determine quais dados devem ser portados, ou seja, se serão dados fornecidos, observados e inferidos objeto deste direito. Por exemplo, é mais eficaz transferir somente pacotes de dados brutos, já que não

	acompanham as regras de inferência. Por sua vez, realizar a transferência de dados gerados por soluções personalizadas é mais complexo, uma vez que são utilizadas regras específicas num cenário que podem não estar presentes em outros. O segundo desafio consiste na segurança no âmbito da transferência dos dados. A título exemplificativo, recomenda-se o uso de criptografia para que não haja intercepção durante o tráfego. Nesse ponto, existe ainda outra problemática em torno da responsabilidade civil daquele que realiza a transferência, o qual deve assegurar que os dados cheguem ao destino com qualidade, sem que sejam corrompidos. Por fim, o maior desafio envolve a questão da interoperabilidade. Os sistemas de armazenamento e processamento de dados não se comunicam, pois não há um padrão definido. Inclusive, uma das propostas aventadas é o desenvolvimento de um conversor que consiste em uma plataforma que entenda os diferentes padrões e realize a conversão entre eles. Em síntese, persistem diversos desafios técnicos na computação a serem enfrentados para que seja possível a concretização do direito à portabilidade. Muito se discute ainda sobre a melhor forma de garantir a segurança dos dados enquanto trafegam, os chamados dados dinâmicos. Dessa forma, entendemos que os desafios da portabilidade para as pequenas empresas serão mais bem delineados a partir da consolidação, por parte da ANPD, dos padrões e diretrizes para o exercício deste direito. No atual cenário, as dificuldades vislumbradas para os Agentes de Tratamento em empresas de pequeno porte são ainda imensuráveis, sendo imprescindível regulamentação para endereçarmos as estratégias adequadas à realidade técnica e financeira destes Agentes.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	O *Sandbox*, método comumente utilizado pela Tecnologia da Informação, e que foi acolhido recentemente pelo Banco Central (Bacen), tem como objetivo a criação de um espaço seguro para o teste de soluções inovadoras com clientes reais. De acordo com o Bacen, o *Sandbox* Regulatório tem por premissa a criação de *"espaços experimentais, que permitem a empresas inovadoras operar temporariamente, dentro de certas regras que limitam aspectos como o número de usuários ou o período no qual o produto pode ser oferecido."*

	Sugerimos a utilização da metodologia de *Sandbox* para o desenvolvimento de aplicações web vinculadas ao Portal do Empreendedor ou mesmo para o desenvolvimento do site da ANPD com todas as funcionalidades necessárias para instrumentalizar as disposições descritas na Lei nº 13.853, de 8 de julho de 2019 de criação da Autoridade. As contribuições adicionais para essa seção podem ser consultadas nas páginas 32 e 33 do Material de Apoio a Tomada De Subsídios Nº 1 /2021.

SUGESTÃO DE NORMATIVO, SE HOUVER

Este normativo regulamenta o art. 55-J, XVIII da Lei Geral de Proteção de Dados (LGPD), que determina a competência da Autoridade Nacional de Proteção de Dados (ANPD) para *"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"*

1. A pessoa física que trata dados com finalidade econômica, incluindo os microempreendedores individuais, ficam dispensados da nomeação de encarregado pelo tratamento de dados pessoais e da elaboração de registro das operações de tratamento de dados pessoais, exceto se tratar dados sensíveis, utilizar inteligência artificial e ou realizar tratamento de dados em larga escala.

2. A microempresa fica dispensada da nomeação de encarregado de proteção de dados. Quanto ao registro das operações de tratamento de dados pessoais, o lançamento fica sujeito à disponibilização, pelo poder público, de mecanismo facilitado, com suspensão da exigência de elaboração até implementação e tempo hábil para adequação, exceto se tratar dados sensíveis, utilizar inteligência artificial e ou realizar tratamento de dados em larga escala.

3. A Empresa de Pequeno Porte com faturamento maior que R$ 180.000,00 até R$ 720.000,00 fica dispensada da nomeação de encarregado de proteção de dados. Além disso, a exigência de registro das operações de tratamento de dados pessoais só poderá ser feita 01 (um) ano após o início da vigência das sanções administrativas.

4. A Empresa de Pequeno Porte com faturamento maior que R$ 720.000,00 só poderá ser exigida no tocante à nomeação de encarregado pelo tratamento de dados pessoais e do registro das operações de tratamento de dados pessoais 01 (um) ano após o início da vigência das sanções administrativas.

5. Todas as sanções administrativas aplicáveis devem ser precedidas de notificação prévia e concessão de prazo para adequação, com indicação específica dos fatores a serem corrigidos, disposição que se aplica a pessoas físicas, inclusive MEI, bem como microempresas e empresas de pequeno porte, independentemente do faturamento.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Confederação Nacional da Indústria (CNI)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	A Lei Geral de Proteção de Dados Pessoais (LGPD) tem como objetivo proteger o indivíduo, o titular das informações. A premissa básica para a criação de uma lei de proteção de dados pessoais é a possibilidade de existir um dano ao indivíduo por meio do uso dos seus dados. Nem todas as empresas tratam o mesmo volume de dados ou oferecem o mesmo grau de risco, em função, por exemplo, da natureza dos dados tratados Se o objetivo da lei é proteger o indivíduo e se as atividades empresariais oferecem graus diferentes de risco e de volume de dados tratados, é razoável que a lei trate diferentes atividades e empresas de forma diferente. A LGPD determina que a Autoridade Nacional de Proteção de Dados (ANPD) edite 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.

	O tratamento simplificado para MPEs é também previsto em legislações internacionais, como na Europeia[1]. Entre as indústrias de menor porte, de modo geral, o tratamento de dados não representa a atividade principal da empresa. Com um volume baixo, muitas vezes coletados apenas por obrigações legais (por exemplo, dados de saúde coletados durante o exame admissional), as empresas não oferecem riscos que justifiquem o tratamento legal idêntico àquele das grandes empresas. De acordo com estimativas divulgadas pela mídia[2], o salário de um encarregado gira em torno de R$ 20 mil e o custo total, incluindo encargos trabalhistas, pode superar os R$ 360 mil por ano, valor equivalente ao teto de faturamento anual de uma microempresa no Brasil. A nomeação de um encarregado é um exemplo, entre outros, que pode onerar excessivamente esse grupo de empresas. Sugere-se que, além da dispensa da nomeação do encarregado, a ANPD estabeleça prazos maiores para o cumprimento de obrigações pelas MPEs; dispense as MPEs do cumprimento de determinadas obrigações, quando a atividade não apresentar alto risco para os direitos e liberdades dos indivíduos, seja pelo porte da empresa ou pelo volume de operações de tratamento de dados e sua natureza; adote etapas de informação e orientação às MPEs como procedimento anterior à aplicação das sanções administrativas; adote critérios específicos para MPEs, com previsões de atenuantes, no âmbito das metodologias que orientarão o cálculo do valor-base das sanções de multa. As dispensas de determinadas obrigações, além de promover a desoneração de empresas que não oferecem riscos aos titulares de dados, permitirá que a ANPD se concentre nos casos de relevo. Esse tipo de abordagem já existe no ordenamento brasileiro, por exemplo, o valor mínimo de faturamento para as análises a serem submetidas ao controle prévio do Conselho Administrativo de Defesa Econômica (CADE)[3].

[1] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. Considerando: (13) Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controlo, são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento.

[2] Época Negócios. Saiba como se tornar um Data Protection Officer, nova profissão em alta no Brasil. Disponível em <https://epocanegocios.globo.com/Carreira/noticia/2019/10/saiba-como-se-tornar-um-data-protection-officer-nova-profissao-em-alta-no-brasil.html>.

[3] LEI Nº 12.529, DE 30 DE NOVEMBRO DE 2011. Art. 88. Serão submetidos ao Cade pelas partes envolvidas na operação os atos de concentração econômica em que, cumulativamente:

Existem sugestões para endereçamento do problema?	**Encarregado** Sugere-se que, para as microempresas e pequenas empresas, startups, empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, seja dispensada a obrigatoriedade legal de indicação de um encarregado de dados. A obrigação se mostra excessivamente onerosa e injustificável quando a atividade não oferece riscos ao titular dos dados. A dispensa da indicação do encarregado não afetará a responsabilização da empresa em casos de violação de direitos do titular. Mesmo sem um encarrado de dados, sempre haverá um representante legal da atividade empresarial. Entre as indústrias de menor porte, de modo geral, o tratamento de dados não representa a atividade principal da empresa. Com um volume baixo, muitas vezes coletados apenas por obrigações legais (por exemplo, dados de saúde coletados durante o exame admissional), as empresas não oferecem riscos que justifiquem o tratamento legal idêntico àquele das grandes empresas. Reconhece-se que, em caráter extremamente excepcional, é possível haver MPEs no setor industrial que tratem dados intensivamente. A fim de evitar distorções indevidas na dispensa, sugere-se a adoção de um modelo semelhante ao europeu, que condiciona a nomeação de um encarregado ao tratamento de dados em grande escala[4]. **Registro das operações de tratamento de dados pessoais**

I - pelo menos um dos grupos envolvidos na operação tenha registrado, no último balanço, faturamento bruto anual ou volume de negócios total no País, no ano anterior à operação, equivalente ou superior a R$ 400.000.000,00 (quatrocentos milhões de reais); e II - pelo menos um outro grupo envolvido na operação tenha registrado, no último balanço, faturamento bruto anual ou volume de negócios total no País, no ano anterior à operação, equivalente ou superior a R$ 30.000.000,00 (trinta milhões de reais).

[4] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 Artigo 37.o Designação do encarregado da proteção de dados: 1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que: [...] 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 controlo 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.o e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o.

	Sugere-se que, para as microempresas e pequenas empresas, startups, empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, seja dispensada a obrigatoriedade legal de manter registro das operações de tratamento de dados pessoais. A dispensa pode adotar a abordagem combinada de porte e risco da atividade, também em linha com o modelo europeu[5], que dispensa o registro para empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja categorias especiais de dados específicas. **Relatório de Impacto** Sugere-se que, para as microempresas e pequenas empresas, startups, empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, seja dispensada a obrigatoriedade legal de elaboração de relatórios de impacto. Por se tratar de uma exposição minuciosa de todo o ciclo de vida dos dados e do nível de risco ao qual os titulares estão sujeitos, a elaboração do relatório de impacto pode exigir a contratação de profissionais experientes e que tenham amplo conhecimento do projeto em questão, impondo significativos investimentos em contratação e em treinamentos. Mais uma vez, sugere-se a inspiração no modelo europeu, que condiciona a obrigação ao risco e ao volume da atividade baseada em dados[6]. **Portabilidade** A portabilidade somente será efetiva se existir uma estrutura que permita uma transferência segura e gratuita de dados entre controladores, de acordo com a escolha do titular do dado. Tratando-se de um trabalho técnico e tecnológico, que gera custos, podendo causar prejuízos financeiros às empresas de menor porte, solicitamos a dispensa da obrigação de

[5] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 Artigo 30.o Registos das atividades de tratamento: [...] 5. As obrigações a que se referem os no s 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.o.

[6] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 Artigo 35.o Avaliação de impacto sobre a proteção de dados. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala.

	portabilidade para as microempresas e pequenas empresas, startups, empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos. **Prazos** Sugere-se a adoção de prazos maiores para o cumprimento de obrigações pelas empresas de menor porte balizados nos prazos concedidos às empresas de maior porte. A exemplo dos prazos diferenciados concedidos à Administração Pública no âmbito do Código de Processo Civil, a ANPD pode estabelecer que as MPEs gozarão de prazo em dobro para o cumprimento das suas obrigações e manifestações nos processos administrativos, em relação aos prazos concedidos como regra geral. **Orientações, sanções e resolução consensual** Sugere-se a adoção de uma etapa de informação e orientação às MPEs, como procedimento anterior à aplicação das sanções administrativas previstas na lei. Para transmitir efetivamente os valores da proteção de dados, a experiência internacional aponta que as Autoridades de Proteção de Dados (APDs) devem ser educadoras e defensoras da privacidade e, assim, promover a cultura da proteção de dados junto à comunidade regulada. A APD deve disseminar os princípios de responsabilização para educar, envolver e aconselhar a comunidade regulada em conformidade com as leis de proteção de dados. As APDs também devem disponibilizar serviços de informação ao público, sensibilizar e informar os indivíduos sobre seus direitos de privacidade. [...] As necessidades de educação e conscientização são impulsionadas pelo fato de que o descumprimento das normas nem sempre é intencional. Muitas vezes, ele é causado pela falta de conhecimento, compreensão ou conscientização. [...] Uma APD com abordagem proativa e orientada para a educação e conscientização a respeito das normas sobre proteção de dados ajuda a maximizar o cumprimento da legislação[7]. Sugere-se a adoção de critérios diferenciados para MPEs no âmbito das metodologias, que orientarão o cálculo do valor-base das sanções de multa, com a previsão de atenuantes. No intuito de estimular a resolução consensual entre as partes, sugere-se a obrigatoriedade de uma etapa de auto composição prévia.

[7] Confederação Nacional da Indústria Em busca de soluções : atributos de autoridades de proteção de dados eficazes. Disponível em <http://www.portaldaindustria.com.br/publicacoes/2017/8/em-busca-de-solucoes-atributos-de-autoridades-de-protecao-de-dados-eficazes/>.

Quais são as oportunidades relacionadas ao tema?	Para a CNI, a LGPD é uma conquista normativa. A atuação da ANPD será fundamental para termos uma aplicação da lei que harmonize os interesses nacionais, o direito à privacidade e para criar condições para o desenvolvimento de novos modelos de negócios que envolvam dados.
Quais são as experiências internacionais sobre o tema?	**União Europeia** Como regra geral, a aplicação do regulamento de proteção de dados guarda relação com a natureza das operações de tratamento de dados. Atividades que apresentam alto risco para os direitos e liberdades dos indivíduos desencadeiam a aplicação de determinadas regras. Como exceção, algumas das obrigações podem não se aplicar às pequenas empresas. Por exemplo, empresas com menos de 250 funcionários não precisam manter registros de suas atividades de processamento, a menos que o processamento de dados pessoais seja uma atividade regular, represente uma ameaça aos direitos e liberdades dos indivíduos ou diga respeito a dados confidenciais ou registros criminais. Da mesma forma, as MPEs só terão que nomear um oficial de proteção de dados se o processamento for seu negócio principal e representar ameaças específicas aos direitos e liberdades dos indivíduos (como monitoramento de indivíduos ou processamento de dados confidenciais ou registros criminais), em particular porque é feito em grande escala. **Austrália** A maioria das pequenas empresas não é alcançada pela Lei de Privacidade de 1988 (Lei de Privacidade). Aquelas que o são ficam obrigadas a cumprir os Princípios de Privacidade da Austrália (Australian Privacy Principles APPs). Uma pequena empresa é aquela com um faturamento anual de $3 milhões ou menos. O faturamento anual para fins da Lei de Privacidade inclui todas as receitas de todas as fontes. Para as empresas abaixo desse valor de faturamento, a incidência da Regulação de Proteção de Dados vai depender do tipo de negócio que é desenvolvido por cada uma. A Lei de Privacidade incide, portanto, sobre os seguintes tipos de negócio: (i) provedor de serviços de saúde, (ii) empresas que lidam com negociação de informações pessoais, (iii) empresa que fornece serviços sob um contrato da Commonwealth, (iv) operador de um banco de dados de locação residencial, (v) órgão de relatório de crédito, (vi) entidade relatora para os fins da Lei de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo de 2006 (vii) associações de funcionários registradas ou reconhecidas pela Lei de Trabalho Justo (Organizações Registradas) de 2009 (viii) empresa que fornece cédulas de ação de proteção (ix) empresa credenciada no sistema ‘Consumer Data Right’ relacionado a um negócio que a Lei de Privacidade incide, (x) empresa

	prescrita pelo Regulamento de Privacidade de 2013, e (xi) empresa que optou por ser coberta pela Lei de Privacidade. **Colômbia** A questão da privacidade e proteção de dados é regida por quatro regulamentações: o Decreto 1.377/13, a Lei 1.581/12, a Lei 1.273/09 e a Lei 1.266/08. O Decreto 1.377 fala sobre consentimento do titular, transferências internacionais de dados e políticas de processamento de dados pessoais. Enquanto isso, a Lei 1.581 estabelece o direito de cada indivíduo de determinar como seus dados serão coletados, armazenados, usados, processados e transferidos — além de regulamentar os direitos à privacidade na coleta e processamento de dados pessoais. A Lei 1.273, por sua vez, traz diretrizes sobre crimes cibernéticos e estabelece que roubar, vender ou comprar dados pessoais é uma atividade criminosa. Finalmente, a Lei 1.266 fala sobre a privacidade de dados no que tange a dados comerciais e financeiros. A Colômbia retirou para micro e pequenas empresas a obrigação de Registro no RNBD (Registro Nacional de Base de Datos). De acordo com o que estabelece o Decreto 090 de 18 de janeiro de 2018, não são obrigados a efetuar o Cadastro empresas e entidades sem fins lucrativos que tenham patrimônio total inferior a 100.000 Unidades de Valor Tributário (UVT). O Registro Nacional de Base de Datos - RNBD - é o diretório público das bases de dados sujeitas a tratamento em funcionamento no país, administrado pela Superintendência da Indústria e Comércio e livremente consultado pelos cidadãos.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	O critério para definição de agentes de tratamento de dados de pequeno porte deve ser aquele da definição de microempresa e de empresa de pequeno porte do Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte (Lei Complementar nº 123, de 14 de dezembro de 2006). A definição de agentes de tratamento de dados de pequeno porte pode, eventualmente, ser complementada por critérios relativos ao volume e à natureza dos dados tratados, bem como, ao número de funcionários de uma empresa.
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)?	Como regra geral, a aplicação do regulamento de proteção de dados guarda relação com a natureza das operações de tratamento de dados. Atividades que apresentam alto risco para os direitos e liberdades dos indivíduos desencadeiam a aplicação de determinadas regras. Como exceção, algumas das obrigações podem não se aplicar às pequenas empresas. Por exemplo, empresas com menos de 250 funcionários não precisam manter registros de suas atividades de processamento, a menos que o processamento de dados pessoais seja uma atividade regular, represente uma ameaça aos direitos e liberdades dos indivíduos ou diga

	respeito a dados confidenciais ou registros criminais. Da mesma forma, as MPEs só terão que nomear um oficial de proteção de dados se o processamento for seu negócio principal e representar ameaças específicas aos direitos e liberdades dos indivíduos (como monitoramento de indivíduos ou processamento de dados confidenciais ou registros criminais), em particular porque é feito em grande escala.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	A obrigação se mostra excessivamente onerosa e injustificável quando a atividade não oferece riscos ao titular dos dados. De acordo com estimativas divulgadas pela mídia recentemente, o salário de um encarregado gira em torno de R$ 20 mil e o custo total incluindo encargos trabalhistas, supera os R$ 360 mil por ano, valor equivalente ao teto de faturamento anual de uma microempresa no Brasil.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.
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?	Nem todas as empresas tratam o mesmo volume de dados ou oferecem o mesmo grau de risco, em função, por exemplo, da natureza dos dados tratados Se o objetivo da lei é proteger o indivíduo e se as atividades empresariais oferecem graus diferentes de risco e de volume de dados tratados, é razoável que a lei trate diferentes atividades e empresas de forma diferente.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.

Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Os custos são ligados, por exemplo, à implementação da solução de segurança dos dados, à manutenção dos processos, à capacitação dos colaboradores, à contratações de consultores/especialistas, dentre outros.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	A regulamentação da LGPD adequada à realidade das empresas de menor porte.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Nº - Podem usufruir do regime simplificado e diferenciado instituído neste regulamento as microempresas e empresas de pequeno porte, conforme definição da Lei Complementar nº 123, de 14 de dezembro de 2006, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, desde que: I – o tratamento de dados não seja objeto substancial da atividade empresarial; ou, II – o tratamento de dados não seja suscetível de implicar risco para os direitos e liberdades do titular dos dados.	
Art. Nº - As empresas sujeitas a este Regulamento gozarão de prazo em dobro em relação àquele estabelecido para os demais agentes de tratamento, para o cumprimento de obrigações e manifestações processuais administrativas.	
Art. Nº - As empresas sujeitas a este Regulamento ficam dispensadas de: I. Manter registro das operações de tratamento de dados pessoais que realizarem (art. 37 da LGPD); II. Elaborar relatório de impacto à proteção de dados pessoais referente às suas operações de tratamento de dados (art. 38 da LGPD; III. Adotar padrões de interoperabilidade para fins de portabilidade (art. 40 da LGPD); IV. Indicar encarregado pelo tratamento de dados pessoais (art. 41º da LGPD).	
Art. Nº - As empresas sujeitas a este Regulamento podem atender às requisições dos titulares de dados pessoais, descritas no artigo 18º da LGPD, pelo meio que entenderem mais conveniente, seja ele eletrônico, telefônico, presencial ou impresso. § 1º Se o titular exigir a resposta por meio impresso, os custos relativos à impressão e postagem poderão ser cobrados do titular, podendo inclusive o atendimento da requisição ser condicionado à comprovação do pagamento.	

Art. Nº - As empresas sujeitas a este Regulamento serão estimuladas a seguir regras de boas práticas formuladas por Associações, cuja observância, obrigatoriamente, deverá ser considerada como atenuante na eventualidade de aplicação de sanções.
Art. Nº - As entidades de representação da atividade empresarial relacionadas às empresas sujeitas a este Regulamento poderão prestar assessoria e auxiliar na negociação, na mediação e na conciliação de reclamações apresentadas por titulares de dados, ou ainda, na hipótese de determinação oriunda de autoridade pública.
Art. Nº- Antes da aplicação das sanções previstas no art. 52º da LGPD, a ANPD deve adotar etapa educativa e de orientação às empresas sujeitas a este Regulamento, com indicação de prazo para adoção de medidas corretivas. § 1º A etapa prévia educativa consiste em orientações individuais e concretas expedidas pela ANPD diretamente à empresa para que esta possa adotar medidas corretivas em caso de violações à LGPD. § 2º A orientação deve elencar as adequações e medidas a serem adotadas, bem como fixar prazo razoável para o seu cumprimento. § 3º Caso a etapa educativa e de orientação descrita no *caput* já tenha sido aplicada anos últimos doze meses da data da ocorrência da nova infração da mesma natureza, a ANPD deve aplicar a penalidade de advertência (art. 52º, I, da LGPD) antes de qualquer outra sanção descrita no artigo. § 4º A reincidência em qualquer infração da mesma natureza relacionada à LGPD dentro do período de doze meses não permite a invocação do tratamento diferenciado previsto no *caput*.

Tomada de Subsídios 1/2021

Mariana Rielli [redacted]

seg 01/03/2021 20:30

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

[redacted]

1 anexo

010321_Tomada de subsídios 01_ Data Privacy Brasil.pdf;

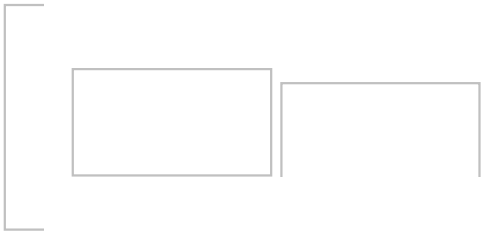
Prezados,

Boa noite. Em anexo, envio a contribuição da Associação Data Privacy Brasil de Pesquisa à Tomada de Subsídios 01/2021. Todas as referências a textos e materiais para consulta estão indicadas nas próprias respostas. Estamos à disposição para conversar sobre quaisquer dúvidas.

Atenciosamente,

--

Mariana Rielli
Líder de Pesquisa
Research Team Leader
[redacted]
www.linkedin.com



MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO:

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de

segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	O principal desafio que enxergamos é o embate entre a necessidade de que (i) a implementação da LGPD não seja uma barreira de entrada aos pequenos empreendedores, ao mesmo tempo em que essa implementação (ii) não seja flexibilizada a ponto de causar danos aos titulares dos dados ou deixá-los desamparados, ampliando sua posição de vulnerabilidade. Nesse sentido, a definição muito abrangente de Pequenas e Médias Empresas e as incertezas acerca da conceituação de startups e empresas de inovação se mostra como um problema para uma regulação que se ampara unicamente nesses conceitos. Justificativa: Essa ponderação surge por conta do reconhecimento acerca da importância das micro e pequenas empresas para a economia brasileira, principalmente em contextos de crise. Isso é claramente demonstrado pelo relatório "Atualização de estudo sobre participação de micro e pequenas empresas na economia nacional (2020)", realizado pelo Sebrae. A título exemplificativo, as MPEs são grandes geradoras de emprego (responsáveis por 51% dos empregos gerados entre 2014 e 2020), bem como uma relevante participação das MPEs no valor adicionado na economia, ou seja, na

	riqueza gerada em cada ano no País. Por isso, entendemos que a implementação da LGPD como uma barreira de entrada aos pequenos e microempreendedores poderia causar efeitos econômicos e sociais indesejados. Nossa abordagem, no entanto, caminha no sentido de uma regulação que deve ser responsiva ao risco - o qual deve ser avaliado, no âmbito da proteção de dados, "[...] não somente como algo que não apenas gera efeitos sancionatórios pela LGPD aos agentes de tratamento que avaliaram o risco de forma errada, mas pode gerar danos aos titulares de dados pessoais, que são os mais vulneráveis nesse contexto''[1]. Por exemplo: riscos de perfilização, discriminação e limitação de direitos e liberdades e "riscos para a segurança dos dados", relacionados a *data breaches*, ataques hackers e acesso não autorizado a dados pessoais transmitidos - como faz o Regulamento Europeu (Regulamento n. 679/2016, GDPR)[2]. Nós entendemos que o risco desses danos decorre diretamente da natureza da atividade da empresa e de operações de tratamento específicas que as empresas podem vir a executar, e não necessariamente no tipo de empresa, seu tamanho ou estrutura. Assim, defendemos que essa preocupação com possíveis danos aos direitos e liberdades dos titulares dos dados não deve ser mitigada por conta da natureza jurídica e/ou tamanho da empresa, sob o perigo de se flexibilizar em demasia a implementação da LGPD, alocando os riscos de danos nas mãos dos mais vulneráveis dessa relação: os titulares dos dados. Nesse sentido, é necessário que a rigidez da regulação seja flexibilizada não somente pela natureza - porte econômico em sentido *lato sensu* - do agente de tratamento, mas que também seja diretamente proporcional aos riscos gerados pela operação. Riscos que, por sua vez, devem estar pautados nos efeitos que podem ser causados aos titulares dos dados (tanto riscos individuais quanto sistêmicos). Para além desse ponto central, pontuamos também algumas preocupações com relação ao tema:

[1] GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 254.

[2] ZANATTA, Rafael. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Encontro da Rede de Pesquisa em Governança da Internet. Rede de Pesquisa em Governança. São Paulo, 2017. p. 11.

	1. <u>Definição muito abrangente de PMEs, startups e empresas de inovação:</u> A definição legal das PMEs, conforme a LC 123/06, abrange diversos setores da economia (serviço, comércio, agricultura) e de diversas escalas. Sendo assim, tratar toda PME sem nenhuma diferenciação poderia gerar um problema ainda maior, no sentido de: (i) deixar titulares desprotegidos por conta de uma flexibilização que abrange setores que desenvolvem atividade de um grau mais elevado de risco; (ii) abrir espaço para manobras de grandes empresas para evadir obrigações de proteção de dados; e (iii) perder uma oportunidade de dinamizar a regulação. Esses pontos serão destrinchados nas questões subsequentes. a. Além disso, a definição de startup e empresa de inovação é um conceito ainda em grande disputa no cenário nacional. A Lei Complementar 167/19 estabelece um parâmetro de autodeclaração no âmbito do sistema do Inova Simples. Já o Marco Legal das Startups, de acordo com o texto atualmente em votação pelo Congresso Nacional, elenca outros critérios como receita bruta e tempo de inscrição no CNPJ. Deste modo, por ainda ser uma questão em aberto, há o risco de se criar ainda mais insegurança jurídica quanto às obrigações relativas à proteção de dados para startups e empresas de inovação. Um movimento de aumento da insegurança jurídica é uma ameaça ainda maior ao ecossistema de inovação no país do que a não flexibilização de obrigações de proteção de dados. 1. <u>Problema de conhecimento sobre LGPD ("Problema de awareness"):</u> Mesmo que o conhecimento acerca da LGPD tenha ganhado força no país, levando as pequenas e micro empresas a saber de sua existência e incidência sobre suas atividades, muitas vezes elas podem não ter clareza sobre os caminhos que precisam tomar para se adequar à legislação. Especificamente, por disporem de menos recursos humanos e financeiros para implementar as medidas necessárias ao cumprimento da LGPD, essas empresas têm mais chance de não conseguirem cumprir com as normas. Nesse sentido, há de se ter em mente esse problema de desconhecimento e de oneração dos pequenos e médios acerca da implementação da Legislação. A solução, ao nosso ver, perpassa, em grande medida, pela criação de uma cultura de proteção de dados pessoais, o que demanda tempo, e um auxílio ainda maior para as pequenas e médias empresas, o que pode ser feito por meio de guias, *templates*, orientações e programas de conscientização, inclusive pela ANPD, no âmbito de competência prevista no art. 55-J, VI da LGPD.

	1. <u>Necessidade de se criar um ecossistema regulatório que fomente a inovação</u>: O fomento da inovação não se deriva de uma ausência de regulação, mas sim de uma regulação que incentive boas práticas de seus agentes e seja responsiva. Argumentamos aqui por um entendimento que as obrigações trazidas pela Lei Geral de Proteção de Dados não representam necessariamente uma barreira a essa inovação, visto que a conformidade com a legislação traz ganhos significativos não só para os titulares de dados, mas também para os agentes de tratamento. **Referências Bibliográficas:** GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271. ZANATTA, Rafael. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Encontro da Rede de Pesquisa em Governança da Internet. Rede de Pesquisa em Governança. São Paulo, 2017. SEBRAE - Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. Atualização de estudo sobre participação de micro e pequenas empresas na economia nacional. FGV Projetos, 2020.
Existem sugestões para endereçamento do problema?	A partir dos principais desafios e problemas identificados (pergunta 01), recomendamos que o risco da atividade desenvolvida pelo agente seja um fator considerado na flexibilização de obrigações. Para isso, recomenda-se que a Autoridade Nacional de Proteção de Dados trabalhe a ideia de risco não a partir de um rol taxativo de atividades de alto risco e nem uma definição fechada, mas sim definindo parâmetros e critérios que podem ser usados para uma avaliação de risco. A realização de estudos de caso mostra-se como uma boa medida para isso, possibilitando uma comunicação dinâmica, transparente e de mais fácil entendimento para um tema complexo. <u>Justificativa:</u> Considerando o enfoque não só no porte econômico em sentido *latu sensu* do agente de tratamento, mas levando em conta também os riscos da atividade por ele desenvolvida, sob a ótica de proteção de dados, é importante que sejam estabelecidos alguns critérios mínimos de análise.

	Para tanto, podem ser realizados estudos de caso analisando empresas de diferentes portes, com diversos graus de risco em sua atividade (padarias, empresas de logística e até startups que utilizam dados de saúde, por exemplo), dando maior concretude para uma regulação flexível. Isso porque, com a realização de estudos de caso, é possível indicar com mais clareza quais tipos de operações de tratamento de dados pessoais podem representar um alto risco[3]. A título de exemplo, podemos citar a recentemente publicada *Guideline* 01/2021 - *Examples regarding Data Breach Notification,* publicada pela European Data Protection Board (EDPB), a qual promove uma análise de incidentes de violações da proteção de dados pessoais, justamente por meio do estudo de diversos casos práticos. Nesse sentido, operações que apresentam alto risco são aquelas que podem impactar de forma significativa as liberdades civis e os direitos fundamentais dos titulares de dados. Assim, se uma operação de tratamento possui um grande volume de dados provenientes, por exemplo, de crianças, ou mesmo dados atrelados à saúde - que são classificados como sensíveis -, pode ser qualificada como de alto risco[4]. Diante disso, surgem questionamentos do que efetivamente poderia ser entendido/abarcado pelo significado de "risco" em tais contextos. A LGPD não trouxe um conceito fechado e específico para a expressão, não sendo igualmente adequado que a ANPD o estabeleça. Isso porque, acreditamos que o foco deve ser voltado para demonstrar que o entendimento acerca do risco deve ser verificado por meio de metodologias de avaliação, além de relatórios de impacto à proteção de dados pessoais. Outro ponto que deve ser levado em consideração é que a análise de risco não pode ser baseada apenas em obrigações gerais da LGPD, sendo uma espécie de tentativa de cumprir com o máximo de obrigações, para demonstrar conformidade com a legislação. A análise deve ter seu foco nas possíveis implicações que o tratamento pode ocasionar aos titulares de dados, se afastando da ideia de ser um simples "checklist de compliance".

[3] GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 264.
[4] Ibid.

	Por fim, importante se faz destacar que não é recomendável que as operações de tratamento de dados que envolvam alto risco sejam classificadas por meio de um rol taxativo. Isso porque, existem grandes possibilidades que muitas operações não estejam acobertadas por uma orientação, simplesmente porque casos semelhantes não foram previamente mapeados e analisados ou sequer já existiram[5]. **Referências Bibliográficas:** European Data Protection Supervisor (EDPS), 2021. *Guideline* 01/2021 - Examples regarding Data Breach Notification. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf. Acesso em 24/02/2021. GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em 24/02/2021. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271. ZANATTA, Rafael. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Encontro da Rede de Pesquisa em Governança da Internet. Rede de Pesquisa em Governança. São Paulo, 2017. QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. In European Journal of Risk Regulation. Vol. 9:3, 2018. p. 502-526.

[5] Ibid.

	GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017). Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917302698. Acesso em 22/03/2020.
Quais são as oportunidades relacionadas ao tema?	Para além da criação de um modelo regulatório flexível que não inviabilize a operação de empresas de pequeno e médio porte e fomente a inovação significativa, enxergamos no tema uma oportunidade da ANPD continuar a modernização da legislação a partir de uma ótica de regulação de risco, que, de maneira geral, busca prevenir os danos *antes que ocorram,* ao invés de focar em sua reparação posterior[6]. Assim, sob essa lógica de regulação *ex-ante*, tem-se a criação de regras e padrões de conduta baseados na qualificação de riscos aos direitos e liberdades dos titulares dos dados pessoais, visando a modificação de comportamentos potencialmente danosos a fim de se evitar esses danos - muitas vezes irreversíveis[7]. Assim, nos parece uma oportunidade fundamental para a ANPD firmar um entendimento de que a parametrização de uma regulação assimétrica no campo da proteção deve observar ao menos duas variáveis que são **cumulativas**: **i)** o porte econômico do agente de tratamento de dados e; **ii)** o risco da sua atividade de tratamento de dados. Com isso, critérios para definir o que é alto, médio ou baixo risco de uma atividade de tratamento de dados são pressupostos estruturantes para traçar o regime diferenciado-assimétrico em questão em proteção de dados, estabelecendo diretrizes gerais sobre o tema, bem como metodologias e indicadores. Justificativa: Atentando ao que dissemos na questão anterior (2), no sentido de que não é benéfico estabelecer um conceito fechado de risco, nem um rol taxativo de quais situações apresentam alto risco, esse tema gera uma oportunidade para a ANPD estabelecer uma orientação e entendimento sobre o tema da regulação sob o enfoque do risco, baseado em métodos científicos de avaliação do risco. Ao

[6] ZANATTA, Rafael. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Encontro da Rede de Pesquisa em Governança da Internet. Rede de Pesquisa em Governança. São Paulo, 2017. P. 188.
[7] Ibid.

	aplicar esses métodos em estudos de caso, é possível obter uma análise mais concreta de quais operações apresentam alto risco, orientando os regulados de maneira mais clara e objetiva. Dessa forma, será viável traçar diretrizes gerais que criem alicerces na avaliação de risco à luz do sistema de proteção de dados brasileiro[8]. É uma circunstância propícia para que a Autoridade demonstre como o risco pode ser avaliado através de metodologias próprias para avaliação de risco e elaboração de relatórios de impacto à proteção de dados pessoais. Também é uma chance para que a agência estabeleça indicadores atribuíveis ao risco, como "alto, médio e baixo" - mas não um valor quantitativo (como afirmar que um agente de tratamento trabalha com 10% de risco em suas operações). É viável, no entanto, ranquear as operações de tratamento de dados, classificando riscos de um 1-100, ou 1-10, por exemplo. Ranquear é diferente de quantificar[9]. A ideia é "[...] orientar no sentido que cada agente de tratamento possa avaliar risco através de indicadores previstos [...]. São os indicadores aplicados na metodologia que contribuem para uma avaliação e conclusão de que determinada operação de tratamento apresenta um alto risco"[10], uma vez que o gerenciamento de risco pode ser resumido a método e a procedimento[11]. Ainda que não seja possível (e nem desejável) ter uma fórmula padrão para todos os agentes de tratamento de todos os setores, entendemos ser necessário criar diretrizes gerais que ajudem a tornar esse cenário menos complexo e mais fácil de ser racionalizado e compreendido. (GOMES, 2020. p. 22). Assim, essa nos parece ser uma ocasião favorável para se criar uma regulação dinâmica e responsiva, atentando-se às mudanças fáticas das operações e seus consequentes efeitos aos titulares dos dados. **Referências bibliográficas:**

[8] GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 264.

[9] Ibid, p. 262.
[10] Ibid, p. 264.
[11] Ibid, p. 265.

	GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271. GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017). Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917302698. Acesso em 22/03/2020. QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. In European Journal of Risk Regulation. Vol. 9:3, 2018. p. 502-526.
Quais são as experiências internacionais sobre o tema?	A experiência internacional sugere que a maior questão relacionada à aplicação da legislação de proteção de dados pessoais às PMEs consiste em dois pontos: a) a falta de familiaridade teórica e prática com a proteção de dados e b) os recursos limitados das organizações. De modo geral, faltam às PMEs conhecimentos básicos sobre proteção de dados e consequente aplicação de boas práticas, de modo que o esforço para a adequação a novas diretrizes legais demanda consideráveis alterações na rotina de atividades desempenhadas. Para as PMEs, o limite de recursos acrescenta desafios às mudanças - não raro, estruturais - necessárias, gerando preocupações sobre subsistência e competitividade. Assim, considerando que a adequação às normas de proteção de dados exige das PMEs mais conhecimento e um esforço relativamente maior, as experiências internacionais apontam para autoridades que auxiliam o processo de adequação das PMEs através de guias e outros documentos informativos e, em alguns casos, para a relativização de determinadas normas, desde que se avalie o risco da atividade desenvolvida, para além do porte econômico. Nesse sentido, um relatório publicados pela autoridade belga, em parceria com a Universidade de Bruxelas, aponta para os principais desafios das PMEs no país, quais sejam: (i) colaboração com terceiros, como subcontratado, e a sua identificação como controlador ou operador na cadeia de tratamento de dados e as suas consequências jurídicas para fins de responsabilidade civil e arranjos contratuais que as coloquem em desvantagem manifestamente excessiva; (ii) falta de recursos financeiros para a implementação de medidas e a capacidade de obter informações suficientes; (iii)

	falta de conhecimento sobre os direitos dos titulares dos dados e (iv) desgaste causado por processos administrativos demorados. Nesse sentido, a experiência belga demonstra que, além de apresentar a possibilidade de um regime jurídico diferenciado, as PMEs trazem a demanda de difusão do conhecimento para a formação de uma cultura de proteção de dados pessoais, o que reforça a imprescindibilidade da atuação da Autoridade Nacional de Proteção de Dados para a promoção de conhecimento e acesso à informação e para estimular a adoção de padrões para a execução das atividades que envolvem o tratamento de dados pessoais considerando o porte das instituições (art. 55-J, VI, VII e VIII). Estas são atividades que viabilizam a implementação de políticas públicas que permitam a melhor instrução dos agentes de tratamento de dados (art. 55-J, I, III, XIII, XVIII, XXIII). Essa demanda é reafirmada ao se observar a atividade das principais autoridades de proteção de dadps ("DPAs") europeias com relação às PMEs. As autoridades de proteção de dados da França, Grã-Bretanha, Itália, Suíça e Irlanda já publicaram juntas mais dez documentos com diretrizes interpretativas sobre o RGPD para PMEs. Em linha com o que foi pontuado nessa contribuição, nenhum dos documentos aponta para um tratamento diferenciado da Lei seja parametrizado única e exclusivamente pelo tamanho ou porte da organização. Deve-se considerar, também, se o grau de risco da atividade de tratamento de dados. Tratam-se, portanto, de critérios cumulativos, e não alternativos. É importante enfatizar que, pela experiência europeia e segundo a Contribuição do EDPB Contribuição da EDPB para a avaliação do GDPR sob o Artigo 97, várias empresas privadas estabeleceram uma linha direta para consultas, a fim de estimular o "desenvolvimento ou participação em um projeto financiado pela UE e à organização ou participação em seminários/workshops/formações dirigidos às PME", ratificando a premissa de que o "calo" mais dolorido da adequação das PMEs à legislação de proteção de dados está no nível de aprendizado de conceitos ligados à própria lei. Problema, este, que pode ser certamente amenizado seguindo a experiência das PMEs europeias, que concentraram esforços no processo de aprendizagem e disseminação da cultura da proteção de dados pessoais. A experiência internacional quanto ao desenvolvimento de leis demonstra que a preocupação com a falta de recursos suficientes para atender a exigências legais é uma realidade. Estados Unidos (em

	estados como Califórnia, em que vige a California Consumers Privacy Act - CCPA, e Nova York com legislações como a 23 NYCRR 500 e Stop Hacks and Improve Electronic Data Security Act - SHIELD Act) e Austrália (Privacy Act 1988) são exemplos de territórios em que a receita anual de uma instituição pode ser um fator de desoneração em relação a algum tipo de obrigação legal. Ainda assim, existem outros critérios não diretamente relacionados com os desafios que PMEs têm para garantir o devido *compliance* à legislação local. O número de funcionários costuma ser mencionado como fator em leis americanas e na GDPR (com relação aos registros sobre o tratamento de dados realizados pela empresa). Ressalta-se que, em muitas destas legislações, não há diferenças substanciais no tratamento em relação a PMEs. Em alguns casos, observa-se que as alterações se limitam a retirar total ou parcialmente alguma obrigação, de modo que a lei como um todo não deixa de ser aplicável a estes tipos de organizações.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	A definição de agentes de tratamento de dados de pequeno porte deve considerar o **modelo de negócio ou atividade desenvolvida pelo agente e o grau de risco gerado por essa atividade**. Este elemento é fundamental para a regulação. Vislumbra-se que a **natureza jurídica do agente** pode também ser considerada. Entretanto, há diversas dúvidas e incertezas que precisam ser levadas em consideração para que não se crie um cenário de aumento da insegurança jurídica, ou mesmo um que propicia um incentivo à "evasão regulatória". Justificativa: Inicialmente se faz necessário reforçar que essa regulamentação específica que visa determinar os critérios a serem considerados para a definição dos agentes deve essencialmente trazer mais, e não menos segurança jurídica para as empresas e titulares. À vista disso, sistematizamos **03 (três) possíveis critérios que podem ser considerados**: **(i)** a natureza jurídica do agente; **(ii)** o modelo de negócio ou atividade desenvolvida pelo agente; e **(iii)** operações de tratamento realizadaspelo agente. Também elencamos os principais desafios que podem ser apresentados com a adoção de cada um dos aludidos critérios, propondo respectivas soluções para cada caso.

	O primeiro critério é o de **“natureza jurídica da organização”**, ou seja, a adoção de parâmetros com base no que consta no contrato social do agente, considerando o seu enquadramento, por exemplo, como uma PME ou como uma Startup autodeclarada. Dessa forma, identificamos alguns desafios inerentes a essa abordagem, quais sejam: a. Como mencionado na questão 01 (um), a definição legal das PMEs, conforme a LC 123/06, abrange diversos setores da economia (serviço, comércio, agricultura) e agentes de diversas escalas, sendo um critério com pouca granularidade e que, por este motivo, pode se mostrar inadequado para parametrizar uma regulação assimétrica. Ainda, é notório que não existem critérios fechados na definição de startups, empresas de inovação e iniciativas empresariais de caráter incremental ou disruptivo. Desse modo, a baixa granularidade e a insegurança jurídica acabam sendo um dos principais problemas encontrados em tais classificações, o que torna a adoção do critério (i) “natureza jurídica do agente” eivado de incertezas. Reiteramos, como dito na questão 01 (um), que um movimento de aumento dessa insegurança é uma ameaça ainda maior ao ecossistema de inovação no país do que a não flexibilização de obrigações de proteção de dados. Maculados pelas mesmas incertezas estão as seguintes categorizações: a.1) A Lei Complementar 167/19 que estabelece um parâmetro de autodeclaração no âmbito do sistema do Inova Simples, para aquelas “iniciativas empresariais de caráter incremental ou disruptivo”. Nesse caso a insegurança perpassa: (i) pelo fator de "autodeclaração'', que é subjetivo e nebuloso; (ii) pela utilização de expressões como “caráter incremental” e “disruptivo” que não possuem uma conceituação fechada. a.2) O Marco Legal das Startups, que ainda está em votação no Congresso Nacional, também elenca critérios como receita bruta e tempo de inscrição no CNPJ, gerando ainda um grande debate sobre o tema. Sendo assim, os critérios para definição de startup e empresa de inovação é uma questão ainda a ser definida dentro da própria legislação setorial, sendo imprudente, no momento, criar uma regulação que tenha por alicerce esses conceitos. b. A criação de flexibilizações de obrigações sem muito rigor e sem a adoção de parâmetros confiáveis, pode gerar estímulo para uma espécie de “elisão fiscal” voltada para proteção de dados. Isso porque, pode tornar-se vantajoso a realização de, por exemplo, cisões de grandes

	organizações em organizações menores para alcançarem um regime de regulamentação menos rigoroso, minando um movimento coletivo para a criação de uma cultura de proteção de dados no país. Importante ter um sistema que identifique e analise eventuais movimentos dessa natureza. a. Uma classificação com base em critérios atrelados exclusivamente à natureza jurídica da empresa normalmente não possui relação direta com a atividade praticada, o que pode ocasionar na flexibilização de atividades de tratamento de alto risco. Isso porque, tal tipo de tratamento pode existir em empresas dos mais diversos segmentos e tamanhos. d.1) A título de exemplo, podemos fazer um exercício comparativo considerando três empresas: (i) Uma grande rede de padarias com filiais em alguns estados do Brasil, mas que não desenvolve nenhuma atividade de tratamento de grau elevado de risco; (ii) Uma PME de marketing digital que realiza *profiling* de titulares de dados como modelo de negócio; (iii) Uma startup que trata dados de saúde para fazer precificação de seguro de saúde. Nesses casos, apesar do exemplo (i) ser a maior empresa em relação ao tamanho e natureza jurídica, as outras duas opções acabam representando um risco muito maior no que concerne aos direitos dos titulares, justamente por conta da atividade desenvolvida. d. Uma flexibilização excessiva da regulamentação pode levar a um menosprezo considerável das questões envolvendo a proteção dos dados pessoais, o que vai de encontro ao quanto disposto pela LGPD. Isso porque uma das principais atribuições da autoridade é justamente fomentar a cultura de proteção de dados no país, zelando pela proteção dos dados pessoais (Art.55-J, I da LGPD) e promovendo o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança (Art.55-J, IV da LGPD). d.1) Nesse sentido, um dos principais problemas identificados pela pesquisa denominada “A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos”, realizada em 2019 com algumas empresas de variados tamanhos e segmentos na região do Sul de Minas, foi uma falta de capacitação e orientação em relação aos colaboradores, aparentemente por não elencarem as problemáticas envolvendo segurança da informação e proteção de dados como prioridade.

	A segunda opção de critério é o de **"modelo de negócio ou atividade desenvolvida pelo agente"**, ou seja, a adoção de critérios com base no produto/serviço que aquele agente desenvolve, qual seu modelo de negócio e se ele implica o tratamento de dados sensíveis. O foco da análise é voltado para os riscos que a atividade pode ocasionar para a proteção dos direitos dos titulares. Dessa forma, identificamos que o principal desafio dessa abordagem seria: a. A dificuldade na definição de quais modelos de negócio apresentam maior risco, especialmente em se tratando de contextos com propostas inovadoras, tendo em vista que os riscos ainda podem não ser muito claros. Como **proposta de solução para o mencionado desafio**, pensamos nas seguintes possibilidades: a. Adoção de uma ótica setorial na flexibilização: Agentes de tratamento que exerçam determinadas atividades, como, por exemplo, no setor financeiro, setor de saúde ou setor de marketing digital, podem ser consideradas atividades de risco para proteção de dados pessoais. Dessa forma, com base na atividade setorial de cada agente, ele pode ser abarcado ou não pela flexibilização. a.1) Possíveis critérios para a avaliação do risco da atividade da empresa: (i) Volume de dados tratados. (ii) Variedade de dados tratados. (iii) Se há tratamento de dados sensíveis. (iv) Quem são os titulares de dados (ex: há tratamento de dados de crianças e adolescentes?) (v) Uso de tecnologias inovadoras para atividades que ocasionam riscos sociais ainda desconhecidos. b. Atribuição de uma espécie de "ônus de provar o risco da atividade" para os agentes de pequeno porte. Ressaltamos que o critério primordial continuaria sendo o risco da atividade, entretanto, poderia ser facultado a tais agentes a possibilidade de elaborar uma avaliação de risco atestando que a atividade principal não importa em um alto grau de risco fazendo com

	que a empresa seja abarcada pela flexibilização. Um ponto importante a se considerar é a obrigatoriedade do registro dessa avaliação para que, em caso de fiscalização ou questionamento pela ANPD, este seja apresentado. Por fim, a terceira possibilidade de critério que pode ser adotado é o de **"operações de tratamento realizada pelo agente"**, ou seja, uma avaliação a partir de operações específicas de tratamento de dados pessoais desenvolvidas pelo agente que podem ocasionar danos aos direitos dos titulares. Podemos citar como exemplo, a realização de procedimentos com a adoção de técnicas de *profiling* e a instalação de câmeras com o objetivo de promover reconhecimento facial dos colaboradores e/ou clientes. Destacamos que tal critério está fortemente ligado à necessidade de realização de relatórios de impacto. Assim sendo, identificamos os seguintes desafios: a. Dificuldade de flexibilizar obrigações gerais dispostas pela LGPD, como a indicação de encarregado, ou mesmo as obrigações envolvendo o registro de atividades de tratamento de dados (ambas questões endereçadas adiante na presente contribuição). b. Dificuldade na criação de condições desiguais para agentes de tratamento que, embora não tenham um modelo de negócio pautados exclusivamente em uma atividade de alto risco, possuem alguma atividade de tratamento que apresenta maior risco. Diante de tais fatores, a análise e a criação de obrigações específicas em atividades de tratamento de alto risco pode ser feita via Relatório de Impacto (RIPD), conforme será abordado no respectivo tópico. **Referências Bibliográficas:** GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em 24/02/2021.

	GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271. PIURCOSKY, Fabrício; COSTA, Marcelo; FROGERI, Rodrigo; CALEGARIO, Cristina. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. In: Suma de Negócios Vol. 10 Num. 23 (Julio - Diciembre). Konrad Lorenz Editores. Colômbia, 2019.
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)?	O RGPD em si não apresenta distinção específica em relação às PMEs com base no seu porte. O único artigo que apresenta algum tipo de exceção nesse sentido é o artigo 30, em que empresas com menos de 250 funcionários não precisam manter registros do procedimento de tratamento de dados da mesma forma que outras empresas. No entanto, a regulação europeia não traz nenhuma definição sobre PMEs e não indica outros tipos de tratamento legal diferenciado. Deste modo, sua aplicação, a princípio, valeria a qualquer empresa. Em contrapartida, o artigo 35, da GDPR, prevê a obrigação de elaborar uma avaliação de impacto à proteção de dados pessoais exigida de todas as organizações que executam atividades de risco elevado. Neste caso, não há exceções para PMEs quando as atividades desempenhadas pela organização implicam alto risco à proteção de dados pessoais. A União Europeia tende a atuar, através das *Data Protection Authorities* (DPAs) de cada Estado-membro e dos órgãos unificados, como *European Data Protection Supervisor* (EDPS) e *European Data Protection Board* (EDPB) no sentido de estabelecer diretrizes para a adequação das Pequenas & Médias Empresas (PMEs) com a legislação de proteção de dados pessoais. A Autoridade belga, por exemplo, publicou, nos últimos meses, documentos com perguntas e respostas frequentes entre as PMEs, dando orientação acerca de qual seria a melhor interpretação de diferentes assuntos. Esse também foi o caso da ENISA, Agência da União Europeia para Cibersegurança, que publicou um guia de segurança e tratamento de dados pessoais voltado especificamente às PMEs. A atuação das DPAs se concentra especialmente em conselhos e orientações interpretativas da legislação de proteção de dados pessoais. A Autoridade britânica (ICO), por exemplo, publicou um extenso documento contendo seções sobre conceitos básicos da legislação, como encontrar e utilizar os melhores recursos, os benefícios da lei de proteção de dados, como criar uma política de

	privacidade, etc. O mesmo acontece na DPA francesa (CNIL), na DPA italiana (Garante), entre outras, que também empenharam esforços em colocar a legislação em uma linguagem acessível através de exemplos ligados às atividades cotidianas das PMEs. Em nenhum dos documentos, no entanto, se propõe que exista um regime jurídico diferenciado para esse tipo de organização. Isso corrobora com a resposta da Comissão Europeia à pergunta "Do the rules apply to SMEs?", em que a Autoridade afirma que as regras se aplicam às PMEs, independentemente do seu tamanho, mas dependendo, por outro lado, da natureza da atividade das organizações. Nesse sentido, ainda que uma empresa seja de porte muito pequeno, se sua atividade principal depender do tratamento de dados pessoais, esta deverá se adequar à legislação e eleger um(a) *Data Protection Officer* (DPO). Esse ponto, assim como outras diferenças específicas, serão abordados em outras perguntas. .
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	Assim como no caso dos programas de governança de dados, abordados em pergunta adiante, a melhor prática nesse caso é a indicação de alguns critérios mínimos pela Autoridade, que serão sugeridos adiante, mas que os próprios agentes de tratamento possam desenvolver suas técnicas e metodologias para o registro, adaptados ao seu contexto e capacidades, em uma lógica de regulação responsiva. No caso de enquadramento em situações consideradas de alto risco (com base em critérios previamente mencionados) a Autoridade não deve descartar uma parametrização mais fechada, com indicação, ao menos, de um conteúdo mínimo para o registro, que pode incluir os seguintes elementos: características do tratamento, quais tipos de dados são tratados, finalidade, titulares; fluxo dos dados (fluxos de compartilhamento e transferência, assim como detalhamento dos terceiros com quem os dados são compartilhados) e, por fim, descrição pormenorizada de medidas de prevenção e segurança da informação. Justificativa: Um breve esforço de pesquisa sobre as origens da LGPD revela que, especialmente durante a Consulta Pública do então Anteprojeto de Lei para a Proteção de Dados Pessoais, em 2015, o dever de registro das operações de tratamento de dados pessoais (art. 37 da Lei nº 13.709/2018, art. 40 do Anteprojeto) gerou algumas discussões por parte das entidades e indivíduos que contribuíram com o processo.

	Essas discussões incluíram desde a necessidade, defendida por alguns atores, de definição de prazos e outras questões procedimentais para os referidos registros até a competência do órgão regulador para fazê-lo, passando por um ponto bastante importante para a presente Tomada de Subsídios: a sugestão de inclusão de uma condicionante ao dever de registro, baseada no ''porte econômico'' do controlador e/ou operador sobre o qual recairá tal obrigação[12]. Conforme explorado nas respostas anteriores, a parametrização de uma regulação assimétrica para distintos atores econômicos deve se pautar (não exclusivamente, mas principalmente) em uma análise sobre o risco que as suas atividades de tratamento de dados implicam para os titulares. Não significa dizer que o porte econômico da organização não deva ser levado em consideração (na medida em que isso pode afetar sua capacidade efetiva de estar em conformidade com determinadas previsões), mas que a ele deve se aliar a análise de risco, que pode incluir variáveis como modelo de negócio e atividades específicas de tratamento de dados, que se desdobram, por sua vez, em critérios como a existência de tratamento de dados sensíveis, tomada de decisão automatizada, *profiling*, bem como o volume de dados tratados, etc. A possível flexibilização do dever de registro das operações de tratamento é um ponto em que convergem fortemente os critérios de porte/capacidade econômica e risco atrelado à atividade do agente econômico em questão. Antes de adentrar nesse aspecto, entretanto, é importante compreender qual é o sentido dessa obrigação e como ela se relaciona tanto com os princípios da LGPD quanto com outros elementos centrais da lei, como os direitos dos titulares. A lei brasileira, assim como outras legislações de matriz semelhante, adota uma série de princípios que ''irradiam'' sobre todos os demais dispositivos da norma e, assim, devem reger **todas** as operações de tratamento de dados pessoais sobre as quais ela incide, independente do setor, tipo ou porte da organização. Nesse sentido, destaca-se o princípio da responsabilização e prestação de contas, que materializa uma inclinação geral da norma de atribuir ao agente de tratamento de dados

[12] INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais.** São Paulo, SP, 2016, p.248. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

	a responsabilidade de adotar medidas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas medidas. Trata-se não apenas de cumprir a lei, mas também de ser capaz de demonstrar o seu cumprimento. Um instrumento importante, senão essencial, para a garantia de prestação de contas é justamente o registro das operações de tratamento, na medida em que uma documentação deve ser apta a demonstrar, no mínimo, os fluxos (internos e externos) de tratamento de dados e a sua gestão. Além de facilitar a materialização do princípio da accountability, a criação de registros das atividades de tratamento de dados também cumpre ao menos outras duas funções: a primeira é facilitar o exercício dos direitos dos titulares (especialmente do art. 18). Cita-se, por exemplo, o direito à ''informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados'' (art. 18, VII), elemento que compõe, justamente, o fluxo dos dados pessoais. Ademais, o registro também é um pilar de qualquer programa de conformidade com a LGPD, independente da sua dimensão ou forma e, inclusive, é próximo do processo de mapeamento de dados que faz parte do diagnóstico que todas as entidades devem realizar sob a LGPD[13]. Dito isso, parte-se para considerações sobre o conteúdo desse registro, bem como possíveis exceções/flexibilizações para agentes que se enquadrem nos termos da presente Tomada de Subsídios. A LGPD não determinou a forma ou um conteúdo mínimo para os registros de atividades de tratamento, nem estabeleceu qualquer tipo de exceção ou parametrização para sua exigência. Em sentido contrário, o Regulamento Geral de Proteção de Dados (RGPD) europeu avançou expressamente nas duas frentes: na primeira, estabeleceu que o ''Record of Processing Activities'' (ROPA) deve conter, no mínimo, tipo de dados que a organização trata, a quem eles se referem (titular), fluxos dos dados, isto é, se o tratamento implica compartilhamento com terceiros ou mesmo transferência internacional de dados, etc. Já em relação a exceções, a lei europeia expressamente afasta a obrigação no caso de empresas com menos de 250 funcionários, exceto em três casos: quando os tratamentos realizados tenham alto potencial de resultar em um risco para os

[13] BIONI, Bruno. A obrigação de registro das atividades de tratamento de dados. Série: Impactos operacionais e normativos da LGPD. Agosto de 2019. Disponível em: https://brunobioni.com.br/wp-content/uploads/2019/08/A-obriga%C3%A7%C3%A3o-de-registro-das-atividades-de-tratamento-de-dados.pdf

	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. No caso brasileiro, ao mesmo tempo em que a LGPD não previu nenhuma exceção ao dever de registro, fazendo supor que ela se aplica horizontalmente a todos os agentes, independente de natureza ou porte, ela também não especificou a forma ou conteúdo desse registro, o que foi uma escolha acertada, na medida em que se faz necessária alguma flexibilidade na sua aplicação. Assim como no caso dos programas de governança de dados, abordados em pergunta adiante, a melhor prática nesse caso é a indicação de alguns critérios mínimos pela Autoridade, que também serão sugeridos mais a frente, mas que os próprios agentes de tratamento possam desenvolver suas técnicas e metodologias para o registro, adaptados ao seu contexto e capacidades, em uma lógica de regulação responsiva. A já mencionada similaridade com o próprio mapeamento de dados, passo primordial para a conformidade de qualquer agente, suscita a possibilidade de criação de um método simplificado de registro que evite duplicidades e desperdício de recursos[14], especialmente no caso de pequenas e médias empresas. Além disso, importante destacar que são as próprias atividades de tratamento desenvolvidas e as eventuais operações que envolvam compartilhamento e transferência de dados que irão ditar a complexidade e extensão do registro, sendo ele uma ‘’fotografia em série’’ das operações de tratamento de dados em curso e do seu status jurídico e de segurança da informação. Como dito anteriormente, isso não significa que a Autoridade não possa participar do processo de criação de boas práticas; pelo contrário, ela deve funcionar como um agente orquestrador desse fluxo, e no caso da obrigação de registro de atividades de tratamento de dados, um ponto de partida importante é a disponibilização de modelos, *templates* e estudos de caso sobre a prática do registro, com a diferenciação entre contextos de alto risco e o restante, tendo, ainda, como variável dentro de cada um desses contextos, o porte e capacidade econômica dos agentes. Ainda, no caso de enquadramento em situações consideradas de alto risco (com base em critérios previamente mencionados) a Autoridade não deve descartar uma parametrização mais fechada, com indicação, ao menos, de um conteúdo mínimo para o registro, que pode incluir os seguintes

[14] Ibid.

	elementos: características do tratamento, como dados tratados, finalidade, titulares; fluxo dos dados (fluxos de compartilhamento e transferência, assim como detalhamento dos terceiros com quem os dados são compartilhados) e, por fim, descrição pormenorizada de medidas de prevenção e segurança da informação. **Referências bibliográficas:** BIONI, Bruno. **A obrigação de registro das atividades de tratamento de dados.** Série: Impactos operacionais e normativos da LGPD. Agosto de 2019. Disponível em: https://brunobioni.com.br/wp-content/uploads/2019/08/A-obriga%C3%A7%C3%A3o-de-registro-das-atividades-de-tratamento-de-dados.pdf INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais.** São Paulo, SP, 2016, p.248. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Nos parece que a abordagem mais correta para lidar com essa questão, considerando a combinação dos critérios que propomos na presente contribuição, é focar em dois aspectos: i) a centralidade do tratamento de dados pessoais, independente da natureza jurídica ou porte da empresa e da natureza dos dados pessoais em questão, para o modelo de negócio da empresa e ii) o risco das operações de tratamento não-pontuais empregadas pelo agente (mensurado por parâmetros como existência de tratamento de dados sensíveis ou de crianças e adolescentes, tomada de decisão automatizada, *profiling*, volume de dados tratados, etc). Dessa forma, a indicação formal de encarregado seria obrigatória para qualquer empresa cujo modelo de negócio seja diretamente baseado no tratamento habitual de dados pessoais (triviais ou sensíveis) ou cujas atividades não-pontuais (centrais ao modelo de negócio ou não) impliquem alto risco para os direitos e liberdades dos titulares, a partir dos parâmetros mencionados. Justificativa:

	Assim como no caso do dever de registro das atividades de tratamento de dados (art. 37), a LGPD também se afastou de outras regulações similares, como o RGPD, ao tratar da figura do encarregado, cuja principal função é operar como um ponto de conexão entre os agentes de tratamento, o titular e a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar os membros da entidade em questão acerca de diferentes aspectos da proteção de dados pessoais. A norma europeia, no seu art. 37, especificou as hipóteses em que a indicação de um encarregado (no caso, data protection officer/DPO) é obrigatória, a partir de uma abordagem baseada no risco. Já os dispositivos da LGPD sobre o tema não excepcionam nenhum caso, limitando-se a prever que ''o controlador deverá indicar encarregado pelo tratamento de dados pessoais'' (art. 41), mas abrem espaço para uma regulamentação assimétrica por parte da Autoridade. Nos parece que a abordagem mais correta para lidar com essa questão, considerando a combinação dos critérios que propomos na presente contribuição, é focar em dois aspectos: i) a centralidade do tratamento de dados pessoais, independente da natureza jurídica ou porte da empresa e da natureza dos dados pessoais em questão, para o modelo de negócio da empresa e ii) o risco das operações de tratamento não-pontuais empregadas pelo agente (mensurado por parâmetros como existência de tratamento de dados sensíveis ou de crianças e adolescentes, tomada de decisão automatizada, *profiling*, volume de dados tratados, etc). Dessa forma, a indicação formal de encarregado seria obrigatória para qualquer empresa cujo modelo de negócio seja diretamente baseado no tratamento habitual de dados pessoais (triviais ou sensíveis) ou cujas atividades não-pontuais (centrais ao modelo de negócio ou não) impliquem alto risco para os direitos e liberdades dos titulares, a partir dos parâmetros mencionados. Verifica-se que, a partir dessa divisão, a obrigatoriedade de indicação do encarregado pode vir a atingir também empresas de porte pequeno ou médio, bem como *startups e* empresas de inovação. Isso porque, conforme mencionado previamente, o porte ou natureza jurídica da empresa não determina a criticidade de suas atividades para a proteção de dados pessoais. Dito isso, há dois pontos importantes a serem abordados em relação à concretização dessa obrigação na prática, bem como à conduta das organizações que não venham a ser atingidas por ela.

	Primeiramente, destaca-se que, deflagrada a obrigatoriedade de indicação do encarregado, a forma pela qual a empresa cumprirá esse dever pode variar, inclusive de acordo com sua estrutura e capacidade econômica. Nesse sentido, a LGPD permite que o encarregado seja uma pessoa física ou jurídica, e a prática do mercado contempla uma variedade de tipos de encarregado: desde colaboradores da empresa já integrados à sua equipe fixa até contratações externas e específicas, passando pela figura do chamado ''DPO as a service'', isto é, a terceirização das funções de encarregado por meio de uma contratação externa, de uma empresa especializada ou mesmo escritórios de advocacia. Assim, existe uma certa flexibilidade no cumprimento da obrigação, que pode ser moldada à realidade do agente. Conforme relatório do Centre for Information Policy Leadership (CIPL), em parceria com o Centro de Direito, Internet e Sociedade (CEDIS) do Instituto de Direito Público (IDP)[15] ''e*mbora organizações maiores possam indicar um encarregado com dedicação exclusiva, isto pode não ser possível para outras organizações, tais como PMEs e startups, devido a restrições de recursos. Entretanto, todas as organizações devem alocar a responsabilidade pelo programa de governança de privacidade e proteção de dados pessoais e suas atividades relacionadas a um indivíduo determinado e habilitado, mesmo que ele trabalhe concomitantemente em uma função diferente.''* Nesse sentido, inclusive, um conjunto de microempresas ou pequenos empresários, se reunidos em uma associação, poderiam nomear um mesmo encarregado que estivesse ligado à entidade de classe. É uma forma de escalar o cumprimento de tal obrigação legal para todo o ecossistema, de modo que a sua internalização não se torne uma barreira de entrada, e há menção expressa a essa possibilidade no art. 37 (4) do Regulamento Geral de Proteção de Dados europeu. Em segundo lugar, é importante salientar que, embora a obrigação de nomeação formal do encarregado não se estenda a qualquer entidade que trate dados pessoais, a LGPD continua sendo uma lei horizontal, cujos princípios e outros dispositivos, como os direitos dos titulares, aplicam-se a todos os atores do ecossistema.

[15] CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL); CENTRO DE DIREITO, INTERNET E SOCIEDADE (CEDIS-IDP). **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)**. 2020. P. 8.

	Dessa forma, é importante que a Autoridade encoraje controladores e operadores, com destaque para as pequenas e médias empresas objeto desta contribuição, a desenvolverem seus próprios meios, que podem não passar, necessariamente, pela indicação de um encarregado, mas ainda devem ser aptos a garantir uma comunicação clara e transparente com o titular, bem como orientar seus colaboradores sobre a proteção de dados pessoais, no sentido da criação e consolidação de uma cultura (organizacional e pública) de proteção de dados no país. Em resumo, o objetivo da figura do encarregado é de otimizar processos internos e contribuir com a garantia de conformidade com a norma, mas também de facilitar intercâmbios entre empresas e outras entidades, titulares e a Autoridade Nacional de Proteção de Dados. Acreditamos que se trata de um objetivo que deve ser perseguido, e orquestrado pela Autoridade, independente da obrigação específica de indicação do encarregado. **Referências bibliográficas:** CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL); CENTRO DE DIREITO, INTERNET E SOCIEDADE (CEDIS-IDP). Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD). 2020.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Buscando responder à pergunta formulada de forma objetiva, não há que se falar em impactos da elaboração de relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte visto que, *a priori*, não há uma obrigação geral de elaboração do instrumento. Nas ocasiões em que houver essa obrigação (realização de operação de tratamento de alto risco) **o fato de o agente de tratamento ser de pequeno, médio ou grande porte não se mostra como um elemento relevante de análise**. **A obrigatoriedade nasce da classificação da operação como de alto risco e, não da natureza jurídica do agente de tratamento.** O impacto do relatório sempre tem como referencial a potencial violação dos direitos dos titulares de dados e, não o impacto econômico da elaboração desse instrumento aos agentes de tratamento. <u>Justificativa:</u> Inicialmente, cumpre destacar que relatório de impacto à proteção de dados pessoais é um instrumento previsto pela LGPD (art. 5º, XVII) que tem o papel de “<u>analisar uma operação específica</u>

	ou um conjunto de operações que podem gerar riscos aos direitos dos titulares (arts. 18, 19 e 20, LGPD), direitos fundamentais e liberdades civis (art. 5, CF) e indicar medidas, salvaguardas e mecanismos para prevenir e mitigar estes riscos". Nesse sentido, o relatório de impacto **não se confunde** com um relatório de diagnóstico. Enquanto o primeiro tem como o titular de dados como seu ponto de atenção, isto é, diagnosticar, mensurar e gerenciar os riscos de uma atividade de tratamento de dados em prejuízo do titular; o segundo tem o agente de tratamento de dados como ponto de atenção da análise, isto é diagnosticar, mensurar e gerenciar os riscos de conformidade de uma atividade de tratamento de dados com a legislação e detecta os principais pontos de atenção e traça um plano de ação. Outro ponto importante a se destacar é que o risco que fundamenta o relatório de impacto se distingue do risco do modelo de negócio ou da atividade da empresa. Portanto, o relatório de impacto deve ser entendido como um instrumento que se funda **em uma operação de tratamento de dados específica ou em um conjunto de operações**. Sendo assim, eventuais critérios para fixar sua obrigatoriedade devem levar em conta os riscos **ocasionados pela operação de tratamento.** Ressalta-se que um relatório de impacto pode avaliar também um conjunto de operações no âmbito de um produto ou serviço que apresente um alto risco**.** **A natureza do agente de tratamento, no caso, agentes de pequeno porte, não é um elemento único e nem mesmo preponderante para a determinação da necessidade de elaboração de um relatório de impacto**. Exemplificando: Uma pequena loja de roupas que possui faturamento anual de R$200.000,00 (duzentos mil reais) que trata dados pessoais apenas para a operacionalização de seu empreendimento (registro de clientes, registro de vendas, anotação de contatos de fornecedores, ficha cadastral de funcionários) não desenvolve nenhuma operação de alto risco. Portanto, nenhuma dessas operações requer, a princípio, a elaboração de um relatório de impacto. Contudo, caso essa mesma loja decida implementar um sistema de câmeras de reconhecimento facial, em que são detectadas também emoções dos clientes para aferir se há maior ou menor interesse em determinados produtos, essa operação, em específico, pode representar um alto risco aos direitos e liberdades fundamentais dos titulares. Sendo assim,

	poderia ser necessária a elaboração de um relatório de impacto à proteção de dados para indicar medidas de mitigação e salvaguardas no âmbito dessa nova operação. Ainda, nesse caso, as demais atividades da loja não seriam afetadas e não entrariam no escopo do relatório de impacto. Isso é observado também no cenário internacional. De acordo com o art. 35 da GDPR, o DPIA (Data Protection Impact Assessment) é necessário quando algum tratamento, **principalmente que implique na utilização de novas tecnologias**, seja suscetível de resultar em um alto risco para os direitos e liberdades dos titulares, considerando a sua natureza, escopo, contexto e finalidade. Ainda, o mesmo artigo elenca critérios de práticas que suscitam o uso do relatório, tais como: (i) Uma avaliação sistemática e exaustiva dos aspectos pessoais relativos ao titulares, baseada no tratamento automatizado, incluindo técnicas de *profiling*, que possam interferir nas decisões que produzem efeitos jurídicos relativos ou afetam de forma significativa os titulares de dados; (ii) o tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1 (Dados sensíveis), ou de dados pessoais relativos a condenações penais e infrações a que se refere o artigo 10.º ; (iii) um monitoramento sistemático em grande escala de uma área acessível ao público. Além disso, destacamos que o *Article 29 Working Party* elaborou o documento "*Guidelines on Data Protection Impact Assessment* (DPIA)", ratificado pelo European Data Protection Board, no qual buscou estabelecer parâmetros e discussões mais aprofundadas, com o objetivo de compreender quais os tratamentos que "provavelmente podem resultar em alto risco". Nesse sentido, o documento destaca que o rol trazido pelo artigo 35 não seria exaustivo, elencando outras 09 (nove) operações que também podem ocasionar "alto risco" (e.g. tratamento de dados genéticos, monitoramento extensivo de funcionários). **Tanto no texto da GDPR, quanto nas orientações do Article 29 Working Party, a natureza jurídica do agente não foi elencada como critério para definir obrigatoriedade ou não do DPIA.** Portanto, conclui-se que existem várias metodologias que a Autoridade Nacional de Proteção de Dados pode adotar, em momento futuro, para tentar definir quais são essas operações de tratamento de maior risco e que ensejariam a elaboração de um relatório de impacto à proteção de dados, mas elas **sempre deverão considerar critérios relativos à operação (ou conjunto de operações) de tratamento, nunca a natureza do agente de tratamento.**

	Referências Bibliográficas: GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em 24/02/2021. GOMES, Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD. **Revista da AASP**, n. 144, 2019. Disponível em: https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD. Acesso em 25/02/2021. Article 29 Working Party (A29WP), 2017. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Acesso em 24/02/2021.
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?	As categorias dados sensíveis ou dados de crianças e adolescentes reforçam a ideia de que a análise de risco que permeia toda essa contribuição não é uma análise de risco regulatório cujo único objetivo é facilitar a conformidade dos agentes de tratamento de dados com a lei. Na verdade, no centro de tal abordagem estão os direitos e liberdades dos indivíduos, os titulares dos dados afetados pela sua utilização. No caso de dados sensíveis e dados de crianças e adolescentes, cada um por suas características específicas, estamos falando de risco elevado pois o impacto do tratamento é consideravelmente mais profundo, uma vez que relacionado a aspectos da dignidade humana (que se desdobra, por exemplo, no direito à não-discriminação), e da proteção de indivíduos cujo desenvolvimento é ''absoluta prioridade'', de acordo com a Constituição. O tratamento diferenciado pela LGPD dessas categorias de dados não é trivial e, nesse sentido, a presença deles nas atividades de quaisquer organizações é um dos fatores que pode deflagrar uma classificação de alto risco e gerar consequências como a necessidade de indicação de um encarregado ou o atendimento a critérios mínimos de registro das atividades de tratamento, dentre outras.

	Assim, entendemos como relevante que a autoridade forneça orientações aos agentes, abordando o aspecto diferenciado das categorias enquanto diretamente relacionadas à dignidade humana e, também, clarificando questões como sobre a definição de dado sensível e quais as diferenças em relação às bases legais aplicáveis para essas categorias especiais em comparação aos dados pessoais comuns ou ''triviais''. . Justificativa: Na avaliação de risco de um tratamento de dados, considera-se tanto o volume das informações tratadas, quanto o tipo de dado e do titular. Nesse sentido, o tratamento de dados sensíveis e de crianças e adolescentes implica a necessidade de maiores cuidados dos agentes de tratamento, mesmo quando o volume de informações e estrutura do agente é menor, se em comparação às grandes empresas de tecnologia. Nesse sentido, cabe ainda a ressalva de que certos dados, ainda que não tenham a princípio essa natureza especial, podem vir a ser considerados como tal, a depender do uso que deles é feito no tratamento[16], bem como da característica de hiper vulnerabilidade do seu titular. Diante disso, as normas, orientações e procedimentos simplificados e diferenciados para empresas de menor porte, devem ter em conta não só o tamanho do agente em si, mas o (i) volume de dados por ele tratado, (ii) a qualidade das informações (uso de dados sensíveis, de crianças e adolescentes) e (iii) os potenciais impactos que o tratamento pode ocasionar aos direitos fundamentais, todos estes elementos que compõem uma análise de risco. As implicações sobre os direitos fundamentais são de especial importância. De fato, as considerações sobre a natureza e classificação dos dados conforme a LGPD são uma parte central da análise e ponto de partida para deflagrar uma análise mais detida sobre os possíveis impactos desse tratamento, na prática. Assim, pode-se depreender que o tratamento de grande volume de dados, proveniente de crianças e adolescentes, ou que sejam sensíveis, é possivelmente de alto risco. A conclusão, contudo, não se encerra aí, sendo necessária a análise dos impactos da operação nas liberdades civis e nos direitos fundamentais dos titulares. A questão em jogo é que as metodologias de análise dos riscos podem numericamente informar um ranking das operações de tratamento de

[16] MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Revista da AASP, número 144, novembro de 2019, pp. 47-53.

	dados (riscos de 0 a 100), mas não podem quantificá-lo, porque o risco, da perspectiva dos direitos fundamentais, não pode ser quantificado[17]. Outro ponto importante a ser observado diz respeito à base legal legitimadora do tratamento dessa categoria de dados. Diferentemente de dados pessoais "comuns", a LGPD determina o consentimento como regra para os casos de tratamento de dados sensíveis (Art. 11º, I) e também de crianças e adolescentes, mas há discussão na doutrina e sugestões de interpretações diversas. No caso das crianças e adolescentes, por exemplo, existe a tese de que a aplicação das bases legais deve se guiar sempre pelo melhor interesse do titular[18], o que não necessariamente resulta em exigência (ou validade) do consentimento parental. Trata-se de um ponto relevante sobre o qual a Autoridade deve se debruçar, a fim de fornecer orientações a todos os agentes que fazem uso desse tipo de dado, inclusive pequenas e médias empresas e startups. **Referências bibliográficas:** BIONI, Bruno; FAVARO, Iasmine; RIELLI, Mariana. **O tratamento de dados de crianças e adolescentes pode ser legal?** Observatório da Privacidade e Proteção de Dados. 19 de outubro de 2020. Disponível em: https://www.observatorioprivacidade.com.br/o-tratamento-de-dados-de-criancas-e-adolescentes-pode-ser-legal/ MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Revista da AASP, número 144, novembro de 2019, pp. 47-53. GOMES, Maria Cecília O. **Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados**. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

[17]GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. **In Temas atuais de proteção de dados**. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

[18] BIONI, Bruno; FAVARO, Iasmine; RIELLI, Mariana. O tratamento de dados de crianças e adolescentes pode ser legal? Observatório da Privacidade e Proteção de Dados. 19 de outubro de 2020. Disponível em: https://www.observatorioprivacidade.com.br/o-tratamento-de-dados-de-criancas-e-adolescentes-pode-ser-legal/

Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	A própria LGPD é clara ao franquear a agentes com diferentes modelos de negócio, bem como portes e capacidades econômicas distintas, a possibilidade de adequar seus programas de governança aos seus contextos organizacionais específicos e aos riscos que suas atividades geram. A exemplo do caso dos registros de atividades de tratamento de dados, o papel da Autoridade, nesse caso, deve ser o de orquestrar um movimento que terá como protagonista os próprios agentes de tratamento, que, setorialmente ou por meio de outras associações, desenvolverão boas práticas para a formulação de programas, considerando que eles são um pilar essencial da conformidade com a lei e implementando os requisitos básicos do art. 50, §2º, I. Para tanto, a Autoridade pode disponibilizar templates básicos e estudos de caso, além de ''reconhecer e divulgar'' as boas práticas desenvolvidas pelo mercado, conforme orientação do art. 50, §3º da LGPD. Justificativa: É provável que as microempresas e empresas de pequeno porte terão um maior número de medidas de adequação às normas de proteção de dados se em comparação às organizações maiores, baseadas no exterior, as quais contam com melhores capacidades de alavancar seus programas globais de governança[19]. Ainda assim, como aponta o Centre for Information Policy Leadership[20]: ''*as organizações de todos os tipos, tamanhos, culturas corporativas, setores podem desenvolver e implementar programas de governança da privacidade e proteção de dados pessoais adequados a seu contexto, riscos e objetivos específicos. Embora possa ser mais desafiador para as PMEs implementar um programa completo, elas também podem adotar medidas para organizar e estruturar seus esforços de governança de privacidade e proteção de dados, muitas vezes de forma mais ágil do que organizações maiores, dependendo dos tipos de dados pessoais que tratam*.'' Além disso, a própria LGPD, em seu art. 50º, §2º, I, c, fornece indicações para que o programa de governança "seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à

[19] Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP). Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD). Setembro de 2020, p.04. Disponível em: https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective- regulation.html

[20] Ibid, p. 13.

	sensibilidade dos dados tratados". E, ainda, considera que um programa de governança pode ser formulado individualmente ou por meio de associações, de modo que agentes de tratamento de dados de pequeno porte podem diluir os custos se juntarem esforços para tanto (artigo 50, caput, da LGPD). Mais uma vez, assim como no comentário relativo ao encarregado, tal obrigação legal se torna ''mais leve'', tendo-se em perspectiva a possibilidade de escalá-la a um conjunto de agentes de tratamento de dados que guardam características similares (e.g., associação de pequenos produtores de café orgânico). É interessante assim, que a autoridade forneça orientações para que os agentes consigam implementar seus programas de acordo com as especificidades do tratamento. Ainda que a implementação de um programa de governança de dados represente um desafio (em maior ou menor grau) às empresas de menor porte, é necessária a consideração de que diante o conjunto de obrigações e responsabilidades dos agentes de tratamento de dados, o programa pode ser encarado como um instrumento que ajuda essas empresas a atenderem às disposições da LGPD. A expectativa é de que a implementação de programas de governança possibilite o cumprimento das exigências legais e regulamentares, reduza a exposição ao risco de não-adequação à LGPD, ofereça melhores condições de proteção de dados pessoais aos titulares e evite multas sancionatórias[21]. Em termos econômicos, o Data Privacy Benchmark Study 2020 da Cisco[22] aponta que mais de 40% das organizações, globalmente, estão vendo retornos em dobro do que gastam em privacidade e proteção de dados pessoais. O argumento de que as práticas de governança são positivas na medida que também promovem um ambiente menos propício a abusos e incidentes que possam gerar multas e prejuízos às empresas já era levantado, inclusive, à época das discussões do projeto de lei nº 4.060/2012[23]. Fora a diminuição de gastos com vazamentos e danos reputacionais, se considerarmos que a privacidade é um fator valorizado pelos consumidores, ela pode representar uma vantagem competitiva para aqueles que

[21] Ibid, p. 04.
[22] Cisco Data Privacy Benchmark Study. From Privacy to Profit: Achieving Positive Returns on Privacy Investment. Janeiro de 2020. Disponível em: https://newsroom.cisco.com/press-release- content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2 047256&utm_medium=RSS
[23] BRASIL, Câmara dos Deputados. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012. Relatório: Tratamento e Proteção de Dados Pessoais. Brasília, 2018, p. 42.

	nela investem, principalmente em um mercado altamente baseado no uso, quase que irrestrito, de dados[24]. Assim, a ideia de implementação de programas de governança de dados não deve ser encarada como um desafio desnecessário às empresas de pequeno porte. Pelo contrário, visto que a LGPD, tal como a GDPR, adotou um modelo de metarregulação[25] (sem entrar no mérito de ser este o modelo mais adequado) as medidas de autorregulação dos agentes se tornam um elemento essencial para o funcionamento do sistema regulatório. **Referências bibliográficas:** Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP). **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)**. Setembro de 2020, p.04. Disponível em: https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html Cisco Data Privacy Benchmark Study. **From Privacy to Profit: Achieving Positive Returns on Privacy Investment. Janeiro de 2020**. Disponível em: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2 047256&utm_medium=RSS BRASIL, Câmara dos Deputados. **Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012**. Relatório: Tratamento e Proteção de Dados Pessoais. Brasília, 2018, p. 42. BIONI, Bruno e MONTEIRO, Renato. **Iniciativa privada: regular o uso de dados pessoais é bom para vocês, confiem em mim**. Novembro de 2016. Disponível em: http://renatoleitemonteiro.com.br/papers/iniciativa-privada-regular-o-uso-de-dados-pessoais/

[24] BIONI, Bruno e MONTEIRO, Renato. Iniciativa privada: regular o uso de dados pessoais é bom para vocês, confiem em mim. Novembro de 2016. Disponível em: http://renatoleitemonteiro.com.br/papers/iniciativa-privada-regular-o-uso-de-dados-pessoais/

[25] ZANATTA, Rafael. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 183.

	ZANATTA, Rafael. **Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?** I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 183.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Entendemos como essencial a estipulação de critérios mínimos a serem exigidos a todos aqueles que tratam dados pessoais. Em relação à parametrização de uma regulação assimétrica, entendemos como necessário que se observe cumulativamente: **i)** o porte econômico do agente e; **ii)** o risco da atividade de tratamento. Também, acreditamos ser essencial que a construção de orientações sobre políticas de segurança não seja restrita a medidas técnicas, mas, também, organizacionais. Nesse sentido, recomendamos que os critérios de políticas de segurança venham acompanhados de orientação que tragam melhores práticas de segurança. Justificativa Nos dias atuais a segurança da informação é essencial para os mais diversos setores e portes de organizações, sendo cada vez mais fundamental o desenvolvimento de políticas de segurança claras por todos os agentes da cadeia de tratamento de dados pessoais. É importante destacar que com a informatização quase total das atividades que visam ao tratamento de dados pessoais, praticamente todos os dados tratados são mantidos em sistemas informáticos[26]. Dessa maneira, partimos do pressuposto que grande parte dos agentes que tratam dados pessoais o façam em sistemas informatizados e, portanto, critérios mínimos de segurança devem ser exigidos a todos aqueles que tratam dados pessoais. Ao tratarmos de políticas de segurança, a discussão sobre risco é inerente. É essencial que na construção de parâmetros objetivos relacionados a política de segurança, seja levado em consideração o risco, e não apenas o tamanho da organização. Isso pois, atualmente, existem agentes de pequeno porte que possuem dados pessoais como peça-chave do seu modelo de negócio ou que tratam quantidades massivas de dados. Nesse contexto, uma organização desse tipo necessita da implementação de uma política de segurança robusta e adequada ao risco da sua atividade. É fundamental que, além de se regular a atividade de tratamento de dados, sejam estabelecidos requisitos de segurança adequados a serem

[26] MENDES, Laura Schertel. Segurança da informação, proteção de dados e confiança. Revista de Direito do Consumidor, São Paulo, v. 90, p. 245-260, nov.- dez. 2013, p. 249

	observados pelos agentes de tratamento de todos os portes, de modo a evitar que ocorram vazamentos e consequentes danos aos titulares[27]. Como já abordado no tópico 3 (três) é essencial que a parametrização de uma regulação assimétrica, também no campo das políticas de segurança, observe ao menos duas variáveis que são **cumulativas**: **i)** o porte econômico do agente de tratamento de dados e; **ii)** o risco da sua atividade de tratamento de dados. Também acreditamos ser essencial que a construção de orientações sobre políticas de segurança não seja restrita a medidas técnicas, mas também medidas organizacionais, como a necessidade de treinamentos e atualização em organizações que realizam tratamentos de dados de alto risco. Um exemplo de boa prática e que tem como parâmetro I - o porte, o perfil de risco e o modelo de negócio da instituição; II - a natureza das atividades da instituição e a complexidade dos produtos e serviços oferecidos; e III - a sensibilidade dos dados e das informações sob responsabilidade da instituição é a Resolução CMN n° 4.658/2018 e a Circular do nº 3.909, ambas do Banco Central. Essas resoluções têm como objetivo trazer padrões mínimos para as organizações do mercado financeiro, mas sem deixar de lado variáveis importantes como risco e porte[28]. Outro ponto de atenção é que a obrigação de segurança não é uma novidade no ordenamento brasileiro, visto que já existem previsões legais, portarias, normatizações e *standards* que já preveem a obrigação de segurança em organizações, nas mais diferentes formas, como por exemplo, a Lei 12.414/2011 – a Lei do Cadastro Positivo –, que determina a necessidade de observância de aspectos técnico-operacionais, utilização de certificações de adequação de segurança dos sistemas e também **a política de segurança**. É importante também destacar as normas ISO, como a ISO 27001, conhecida como a única norma internacional auditável que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Nesse sentido, recomendamos que ao estabelecer critérios de políticas de segurança, principalmente para organizações de alto risco e/ou as de pequeno porte, é necessário o desenho e construção de orientação que tragam as melhores práticas de segurança, realizando uma

[27] GOULART, Guilherme Damasio; MENKE, Fabiano. Segurança da Informação e Vazamento de Dados. In: BIONI, Bruno et al (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.
[28] TEÓFILO, Davi et al. LGPD e Fintechs: um novo cenário para o compliance digital. São Paulo: Baptista Luz Advogados, 2019. 44 p. Disponível em: https://baptistaluz.com.br/institucional/lgpd-fintechs-compliance-digital/. Acesso em: 24 fev. 2021.

	diferenciação entre o tipo da organização e o risco da atividade. Isso porque, o risco e a necessidade de uma política de segurança podem variar muito a depender do modelo de negócio: uma startup que trata dados médicos, por exemplo, dependerá de uma política de segurança muito mais robusta que uma mercearia de bairro. Construir orientações que tragam exemplos práticos podem servir como forma de esclarecer e trazer segurança jurídica para organizações de pequeno porte. Destacamos aqui a previsão legal do artigo art. 50, § 1.o, que determina que deverão ser consideradas "a natureza, o escopo, a finalidade e a probabilidade e a **gravidade dos riscos**", enquanto o § 2.o estabelece a observância da "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**". Dessa forma, podemos extrair da análise do texto legal que a elaboração de políticas de segurança deve ter como foco o dano para os titulares de dados e, partir necessariamente, de uma análise voltada para os riscos que a atividade exercida e o ambiente tecnológico estão expostos para definir quais são as medidas necessárias para o seu controle. Acreditamos que políticas de segurança podem fortalecer o princípio da prevenção, criando incentivos para os agentes de diferentes portes possam atuar de forma preventiva durante o tratamento de dados pessoais, construindo parâmetros técnicos e organizacionais que busquem proteger os dados dos titulares de acessos não autorizados. Uma eventual regulamentação da autoridade deve destacar a importância de políticas de segurança para agentes de todos os portes, mas também deve demonstrar que essas políticas de segurança devem ser mais ou menos robustas de acordo com o modelo de negócio e atuação da organização. Por fim, é necessário um equilíbrio entre o que é razoável exigir das organizações e também a importância da segurança para a garantia dos princípios e direitos da LGPD. É essencial que a Autoridade incentive a construção de políticas de segurança e prevenção por todos os agentes, nos mais diferentes portes, já que essa política pode ser crucial para as organizações, principalmente em um contexto de aumento exponencial dos incidentes notificados. **Portanto, acreditamos que a necessidade de políticas de segurança mais ou menos robustas estão associadas ao risco da atividade, não da natureza jurídica do agente de tratamento.** **Referências bibliográficas:**

	MENDES, Laura Schertel. **Segurança da informação, proteção de dados e confiança**. Revista de Direito do Consumidor, São Paulo, v. 90, p. 245-260, nov.- dez. 2013, p. 249 GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** In: BIONI, Bruno et al (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666. TEÓFILO, Davi et al. **LGPD e Fintechs: um novo cenário para o compliance digital**. São Paulo: Baptista Luz Advogados, 2019. 44 p. Disponível em: https://baptistaluz.com.br/institucional/lgpd-fintechs-compliance-digital/. Acesso em: 24 fev. 2021.
Quais são os impactos da implantação de avaliação sistemática de riscos à	Conforme argumentado nas respostas anteriores, eventuais flexibilizações de obrigações da LGPD para agentes de pequeno porte, stratups e empresas de inovação deve, em todos os casos, considerar como um de seus elementos de análiseos riscos apresentados pela atividade do agente. Esses riscos devem ser analisados tanto pela ótica dos direitos fundamentais quanto pela ótica da proteção de dados. Ainda, há de se avaliar os impactos de determinada obrigação trazida pela LGPD não só para os agentes de pequeno porte, mas também, e principalmente, os impactos do não cumprimento dessa obrigação aos titulares de dados, visto que se encontram em posição de vulnerabilidade face aos controladores. Deste modo, a ausência de uma avaliação de risco pode deixar os titulares ainda mais vulneráveis, além de impossibilitar uma parametrização do agente de tratamento, essencial para uma regulação assimétrica. Assim, ao menos em um momento inicial é fundamental que exista uma avaliação dos riscos da atividade do agente para a proteção de dados pessoais e os direitos dos titulares. Caso esses riscos apresentados sejam baixos, é possível que algumas obrigações sejam flexibilizadas, conforme tratado em outros momentos na presente contribuição.

privacidade dos dados aos agentes de pequeno porte?	
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Partimos da perspectiva de que a análise de impacto da implantação da portabilidade deve ter como foco o titular dos dados. Em relação aos impactos, acreditamos que a portabilidade pode ser positiva aos pequenos negócios no campo concorrencial, ao aumentar a possibilidade de novos entrantes em determinados mercados. Também, entendemos que a regulação da portabilidade, principalmente no âmbito das PMEs e Startups, deve pensar a interoperabilidade e sua regulamentação através da construção de critérios objetivos, levando em conta sempre na criação de padrões que contemplem diferentes tipos de organizações e observem a experiência internacional. Justificativa A portabilidade de dados é um direito que busca empoderar os indivíduos e permitir que esses exerçam sua autodeterminação informacional, ao mesmo tempo que é um mecanismo de fomento e promoção da concorrência, que possibilita o exercício do direito de escolha pelo consumidor. Assim, trata-se efetivamente de um espaço de interface entre esses dois campos, incluindo, ainda, a proteção do consumidor[29]. Somado aos outros direitos previstos na LGPD, a portabilidade pode facilitar o livre fluxo informacional ao possibilitar que o titular escolha e determine o agente responsável pelo tratamento dos seus dados[30]. É importante destacar o foco no **titular** dos dados, visto que, mesmo que a portabilidade possa afetar a concorrência, ela surge como uma forma de fortalecer a autodeterminação informativa e não regular propriamente a concorrência, mesmo que traga impactos nesse âmbito. Em síntese, evita-se que os consumidores fiquem presos a determinado ofertante (efeito lock in) em virtude das dificuldades ou mesmo dos altos custos de troca (switching costs) que decorreriam da "perda" dos dados[31]. Dessa forma, como já endereçado nas outras perguntas, acreditamos que a análise de impacto da implantação da portabilidade deve ter como foco o titular, que em circunstâncias em que o direito

[29] PONCE, Paula Pedigoni. Direito à portabilidade de dados:: entre a proteção de dados e a concorrência. Revista de Defesa da Concorrência, [s. l], v. 8, p. 134-176, jun. 2020. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/521/26. Acesso em: 25 fev. 2021.
[30] ZANFIR-FORTUNA, Gabriela. The right to Data portability in the context of the EU data protection reform. International Data Privacy Law, v. 2, n. 3, p. 149–162, 1 ago. 2012
[31] FRAZÃO, Ana. Nova LGPD: direito à portabilidade: a 11ª parte de uma série sobre as repercussões para a atividade empresarial. Jota. 07 jan. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-a-portabilidade-07112018 . Acesso em: 24 fev. 2021.

	seja bem regulamentado poderá determinar se seus dados serão entregues a outras organizações e quais organizações devem receber esses dados. Isso permite que o consumidor se beneficie da economia de custos feita pelas organizações. Ao exercer sua escolha de ocultar seus dados de organizações que fornecem 'ofertas ruins' e optando apenas por fornecê-los a organizações que estendem 'boas ofertas', os consumidores podem exercer pressão positiva sobre os prestadores de serviços para fornecer um produto ou serviço mais competitivo[32]. Em relação aos impactos, no âmbito da concorrência, admite-se impactos positivos do direito à portabilidade já que aumenta a possibilidade de para novos entrantes, principalmente ao pensarmos em agentes de pequeno porte. Isso pois, quanto mais fácil for para o usuário trocar e escolher uma nova empresa ou serviço, maior a possibilidade de conhecer os serviços de um novo agente entrante no mercado. Outro ponto de impacto é que se bem implementada a portabilidade pode trazer mais eficiência para as MEIs e Startups, já que elas podem obter acesso de formas muito mais simples a dados de diferentes titulares. Isso pode, por sua vez, melhorar a capacidade de desenvolvimento e melhorar as ofertas de produtos que são mais bem direcionadas à sua base de clientes, derivando mais informações de um universo mais amplo de dados e clientes. Acreditamos que uma eventual regulação desse direito, principalmente no âmbito das MEI`S e Startups, deve pensar a interoperabilidade e sua regulamentação através da construção de critérios objetivos e que condizem com a realidade e experiência internacional, pensando sempre na criação de padrões de para fins de portabilidade que também contemplem organizações pequenas, startups e MEIs, principalmente pensando no custo para a execução dessas atividades. Para fins de impacto, também sugerimos a elaboração de estudos de caso, que contemplem organizações dos mais variados setores, demonstrando formas práticas e concretas de uso e aplicabilidade desse direito, principalmente em um cenário de MEIs e Startups e que considere os inúmeros modelos de negócio, funcionando com formatos técnicos distintos. Acreditamos que é de suma importância pensar a forma pela qual a interoperabilidade será executada entre bancos de dados de organizações distintas.

[32] THE PERSONAL DATA PROTECTION COMMISSION SINGAPORE (Singapura) (org.). Discussion paper on Data Portability: personal data protection commission in collaboration with competition and consumer commission of singapore. : Pdpc, 2019. 22p.

	Se bem implementado, podemos ter um cenário em que os consumidores se beneficiam de seus direitos à portabilidade de dados, enquanto a concorrência no mercado é reforçada pela existência desse direito. Por outro lado, impor requisitos de portabilidade semelhantes a todas as empresas, independentemente do tamanho, pode resultar em custos de conformidade desproporcionais para as empresas menores que podem não ter o nível necessário de conhecimento ou recursos para desenvolver sistemas que permitam a portabilidade de dados. Isso pode impedir a capacidade das pequenas e médias empresas de competir efetivamente com seus concorrentes maiores. Uma estratégia possível é adotar padrões de dados abertos, amplamente usados e estabelecidos para suportar a portabilidade e reduzir o custo de implementação para os negócios. Exemplo de boa prática é a recente implementação do Open Banking, que vai possibilitar que o cliente seja dono de seus dados financeiros e possa escolher quando e com quais empresas vai compartilhá-los. Por fim, acreditamos a discussão acerca da portabilidade de dados no Brasil precisa dar um passo à frente e sair da discussão teórica, sendo de grande valia debates acerca de como tornar aplicável o direito à portabilidade de dados, e por mais que exista uma aparente boa vontade das empresas em viabilizar essa operação, é necessário o estabelecimento de parâmetros razoáveis a fim de tornar essa, uma prerrogativa viável[33]. **Referências bibliográficas:** PONCE, Paula Pedigoni. **Direito à portabilidade de dados:: entre a proteção de dados e a concorrência**. Revista de Defesa da Concorrência, [s. l], v. 8, p. 134-176, jun. 2020. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/521/26. Acesso em: 25 fev. 2021. ZANFIR-FORTUNA, Gabriela. **The right to Data portability in the context of the EU data protection reform**. International Data Privacy Law, v. 2, n. 3, p. 149–162, 1 ago. 2012 FRAZÃO, Ana. **Nova LGPD: direito à portabilidade: a 11ª parte de uma série sobre as repercussões para a atividade empresarial**. Jota. 07 jan. 2018. Disponível em:

[33]GOMES, Maria Cecília. Portabilidade de dados reputacionais: a problemática da sua aplicabilidade na economia compartilhada. Disponível em: https://www.academia.edu/37027420/Portabilidade_de_dados_reputacionais_a_problem%C3%A1tica_da_sua_aplicabilidade_na_economia_compartilhada

	https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-a-portabilidade-07112018 . Acesso em: 24 fev. 2021. THE PERSONAL DATA PROTECTION COMMISSION SINGAPORE (Singapura) (org.). **Discussion paper on Data Portability: personal data protection commission in collaboration with competition and consumer commission of singapore**. : Pdpc, 2019. 22p. GOMES, Maria Cecília. **Portabilidade de dados reputacionais: a problemática da sua aplicabilidade na economia compartilhada**. Disponível em: https://www.academia.edu/37027420/Portabilidade_de_dados_reputacionais_a_problem%C3%A1tica_da_sua_aplicabilidade_na_economia_compartilhada
	Argumentamos aqui que a Lei Geral de Proteção de Dados traz obrigações que não devem ser vistas como uma barreira à inovação, mas sim como uma janela de oportunidade. Em consonância com as demais questões endereçadas nesta contribuição, vislumbra-se que há sim espaço para flexibilizar algumas obrigações para agentes de pequeno porte, especialmente àqueles que realizam atividades de baixo risco. Contudo, há também um caminho para capacitar esses agentes e difundir uma cultura de proteção de dados. <u>Justificativa:</u> Primeiramente, deve-se ter em mente que entender a Lei Geral de Proteção de Dados como uma barreira à inovação mostra-se como uma abordagem defasada. Ainda que a lei imponha obrigações regulatórias aos agentes de tratamento, um ecossistema que promove e incentiva a inovação não deve ser entendido como um ecossistema ausente de regulação, ou com o mínimo de regulação possível, mas sim como um que possui um *framework* regulatório que possibilita aos agentes realizarem suas atividades incorporando essa regulação à sua realidade e garantindo o respeito aos direitos e liberdades fundamentais dos titulares. Algumas das inovações trazidas pela LGPD, como o direito à portabilidade, tem justamente o intuito de aliar a proteção do titular, conectado especialmente com a ideia de autodeterminação informativa, com o fomento a inovação, reduzindo barreiras de entradas para novos atores e incentivando o incremento a modelos de negócios já existentes.

	Além disso, obrigações que em uma análise apressada poderiam ser entendidas como barreiras à inovação, por gerar um aumento burocrático nas organizações, como por exemplo o dever de manter registro das atividades de tratamento, pode ser entendido, em uma análise mais detida, não só como uma importante obrigação derivada do princípio de prestação de contas, mas também como uma janela de oportunidade para a organização se conhecer melhor e com isso otimizar suas atividades ou até mesmo gerar novos *insights*. A elaboração de um relatório de impacto à proteção de dados previamente à comercialização de um produto ou serviço inovador, que ainda possui riscos sociais desconhecidos, por exemplo, pode servir como importante ferramenta para que a organização mapeie pontos críticos desse produto que poderiam vir a ser questionados futuramente e os resolva preventivamente. Isso pode gerar um benefício não só para os direitos de titulares que viriam a ser afetados, mas também para que a própria organização possa aperfeiçoar seu produto ou serviço. Ainda, os princípios trazidos pela LGPD possuem como foco não só a proteção do titular de dados, mas também a otimização das atividades de uma organização. O princípio da qualidade dos dados, por exemplo (art. 6º, V) mostra-se como um exemplo claro disso. É interessante não só para o titular que seus dados estejam atualizados e corretos, mas também para a organização poder conhecer melhor seus clientes, parceiros ou colaboradores. Sendo assim, argumentamos aqui que abordagem mais moderna para se entender a regulação da proteção de dados é uma que a enxerga como uma janela de oportunidade: “Apesar de uma nova regulação causar receio em relação aos custos de conformidade (o aumento do custo Brasil), a LGPD representa uma janela de oportunidade. Primeiramente, porque as organizações terão de colocar ordem na casa, pois vão precisar conhecer melhor as suas bases de dados e lhes atribuir uma finalidade específica – um dos princípios da lei. É um exercício que poderá trazer insights para se repensar o próprio modelo de negócio ou política pública e para lançar novos produtos e serviços. Em segundo lugar, porque a adequação à legislação pode melhorar a reputação da empresa, na medida em que o tratamento adequado dos dados pode ser explorado no plano de comunicação para reforçar a confiança com o titular da informação. Terceiro, porque a lei traz exigências associadas à segurança da informação no sentido não só de prevenir o vazamento de dados, mas também de remediá-lo da forma mais eficiente caso isso ocorra. Trata-se de medidas cujo saldo final

	pode agregar valor e competitividade a uma organização, a depender de qual mentalidade orientará o seu processo de conformidade" (BIONI, 2019) Essa visão é corroborada por achados empíricos. No relatório "Data Privacy Benchmark Study" de 2021 elaborado pela CISCO, foi evidenciado que 85% das organizações tiveram um retorno positivo do investimento feito na área de privacidade e proteção de dados. 35% delas relataram retorno de pelo menos duas vezes maior do que o valor investido. Dentre os principais benefícios encontrados pelo investimento estão listados os seguintes ganhos: • Tornar a empresa mais atraente • Construção de confiança • Atingir a eficiência operacional • Capacitar a inovação • Mitigação de perdas de segurança • Redução de atrasos nas vendas Sendo assim, há um primeiro alerta para que não se entenda que a promoção e incentivo à inovação está atrelada a uma flexibilização regulatória. **Referências Bibliográficas:** BIONI, Bruno. Inovar pela lei. **GV-executivo**, v. 18, n. 4, julho-agosto, 2019. Disponível em: https://rae.fgv.br/gv-executivo/vol18-num4-2019/inovar-pela-lei. Acesso em 25/02/2021. CISCO. Data Privacy Benchmark Study: Forged by the Pandemic: The Age of Privacy. 2021. Disponível em: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=213931. Acesso em 25/02/2021.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	

Art. Xxxx ....

Tomada de Subsídios 1/2021

Contato ABIPAG <contato@abipag.com.br>

seg 01/03/2021 21:04

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

[redacted]

1 anexo

Abipag - Contribuição Tomada de Subsídios ANPD.pdf;

Prezados, boa noite.

A Associação Brasileira de Instituições de Pagamentos (“ABIPAG”) vem, por meio deste, apresentar suas considerações acerca da Tomada de Subsídios ANPD 01/2021.

Solicitamos, por gentileza, que confirmem o recebimento deste e-mail e nos colocamos à disposição para quaisquer esclarecimentos que se façam necessários.

Atenciosamente,

Associação Brasileira de Instituições de Pagamentos

São Paulo, 1º de março de 2021

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Esplanada dos Ministérios – Bloco C – 2º andar – Brasília – DF

Por e-mail: consultapublica@anpd.gov.br

Ref.: Tomada de Subsídios nº 1/2020

1. A **Associação Brasileira de Instituições de Pagamentos ("ABIPAG")**, inscrita no CNPJ sob o nº 26.425.404/0001-10, tem a missão institucional de representar instituições entrantes no mercado de meios de pagamentos eletrônicos, tais como instituições de pagamento, credenciadoras e emissoras de moeda eletrônica, e instituições financeiras na modalidade sociedade de crédito direto, **sobretudo em prol da promoção da livre concorrência, livre iniciativa e isonomia no mercado.**

2. Por se tratar de um tema de extrema relevância aos seus associados e seus respectivos clientes – usuários finais recebedores de transações de pagamento, a ABIPAG vem, respeitosamente, à presença da Autoridade Nacional de Proteção de Dados ("ANPD"), apresentar suas contribuições à Tomada de Subsídio nº 1/2020, referente à regulamentação da aplicação da Lei Geral de Proteção de Dados Pessoas ("LGPD") para microempresas e empresas de pequeno porte, bem como para iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos ("agentes de pequeno porte").

3. Inicialmente, a ABIPAG gostaria de enaltecer a iniciativa de V.Sas. por se preocuparem em estabelecer, desde o início do processo de regulamentação da LGPD, um diálogo aberto com a sociedade, de maneira a proporcionar um ambiente de maior segurança jurídica, possibilitando que o respeito aos direitos dos titulares dos dados pessoais caminhe *pari passu* com as políticas

públicas que objetivam a transformação digital do país, a partir do desenvolvimento de novos negócios, sobretudo aqueles realizados em ambiente digital.

4. Nessa linha, a ABIPAG manifesta desde logo sua concordância com o posicionamento externado por esta Autoridade em sua Nota Técnica nº 1/2021/CGN/ADPD,[1] ao anotar que a redução da carga regulatória e o estímulo da inovação são fatores fundamentais para o desenvolvimento do País.

5. Por outro lado, a ABIPAG concorda com a ponderação de que fatores como "*o porte de uma empresa não altera[m] o direito fundamental que o titular tem à proteção de seus dados pessoais, nos termos do art. 17 e seguintes da LGPD, nem desobriga[m] que as atividades de tratamento de dados observem a boa-fé e 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*" (fl. 3).

6. À vista das premissas acima, a ABIPAG considera que a flexibilização de obrigações constantes da LGPD como forma de incentivo a novos negócios deve se dar a partir de mecanismos regulatórios que, a um mesmo tempo, promovam grau correto/adequado de proteção dos direitos dos titulares de dados, e viabilizem **a entrada e a competitividade de novos e pequenos negócios**, **possibilitando a diversificação dos serviços prestados e a disrupção de modelos tradicionais**, o que está em linha, aliás, com os comandos da Lei nº 13.874/2019, que instituiu a Declaração de Direitos de Liberdade Econômica.

7. Vale dizer, a regulamentação das obrigações inseridas na LGPD deve levar em consideração aspectos práticos que diferenciam significativamente a atuação de novos negócios e empresas entrantes dos agentes de maior porte já estabelecidos no mercado. O desenvolvimento tecnológico observado no período recente contribuiu para a redução de barreiras à entrada de novos concorrentes, que podem desenvolver e ofertar novos modelos de negócio e soluções inovadoras baseadas em tecnologia, que ampliaram a oferta e a diversidade de serviços em diferentes setores da economia, com evidentes benefícios aos usuários finais e o aumento do dinamismo da concorrência.

8. Especificamente no caso dos serviços financeiros, pode-se destacar aqui o surgimento das *fintechs* e *insurtechs* – segmentos associados à ABIPAG que exploram nichos de mercado outrora não atendidos adequadamente por parte de incumbentes já ativos no setor, resultando em um aumento da complexidade dos ecossistemas relacionados a tais mercados.

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica.pdf.

9. Portanto, entende-se que, se de um lado novas ferramentas tecnológicas permitiram o surgimento de tais agentes, há de se ter em vista, por outro, que por se tratarem de novos entrantes, ao menos em um momento inicial suas operações usualmente são de menor escala e dependem da realização de investimentos significativos para o desenvolvimento de novos produtos e serviços com objetivo de viabilizar suas operações e sua efetiva entrada em diferentes mercados. Nesta condição, sofrem com limitações de ordem financeira, de disponibilidade de recursos humanos e para a estruturação e consolidação de seus modelos de negócios, que devem ser tomadas em conta quando da edição de novos regulamentos que passarão a impactar suas atividades.

10. E tais limitações se ampliaram diante do estado de calamidade pública que se instalou no País em razão da pandemia do coronavírus (COVID-19), que impactou de forma relevante a economia brasileira. Em um cenário de possível e significativa retração econômica, onde pequenos e médios empreendedores estarão especialmente expostos, e muitos deles terão sua própria sobrevivência ameaçada, a adoção de medidas regulatórias assimétricas em relação a novos entrantes se torna fundamental para garantir a tais empresas o tempo necessário para adequação ao ordenamento jurídico vigente, ao mesmo tempo em que não se deixa de tutelar os objetivos visados por meio da LGPD.

11. A ABIPAG entende que estas medidas proporcionarão um aumento da concorrência e da inovação, sem a imposição de custos regulamentares que não se justificariam frente aos riscos oferecidos por modelos de negócios inovadores. É dizer, a isonomia entre participantes do mercado será assegurada justamente pelo tratamento diferenciado entre agentes de diferentes portes, considerando as características de cada tipo de operação.

12. Inclusive, essa tem sido a tendência iniciada a partir de 2013 no setor financeiro e de meios eletrônicos de pagamento, com a edição da Lei nº 12.865/2013, que contribuiu significativamente para a abertura desse mercado a novos concorrentes, bem como por uma série de intervenções regulatórias levadas a efeito pelo Banco Central do Brasil, para a finalidade de viabilizar o surgimento e a permanência de empresas inovadoras neste setor. A esse respeito, pode-se citar a edição de normas regulamentando o denominado Open Banking e o sistema de pagamentos instantâneos PIX como exemplos de medidas recentemente adotadas e que levaram a um aumento da inclusão financeira e da concorrência, com a consequente diminuição da concentração de mercado em torno de um rol limitado de incumbentes.

13. Tendo isto em vista, sugere-se à ANPD o alinhamento de suas políticas públicas àquelas que vêm sendo adotadas pelo Banco Central do Brasil e demais órgãos governamentais de

incentivo a novos negócios, visando a criação de um ambiente mais favorável à inovação e à ampliação da competição.

14. Deve-se ressaltar que não se trata aqui de afastar possibilidade de aplicação da regulação sobre tais agentes econômicos, mas sim de apontar a necessidade de sua adequação frente às características destas empresas, de modo a não serem impostas novas barreiras à entrada e permanência no mercado.

15. Portanto, especialmente para fins da edição de procedimentos diferenciados a determinadas categorias de agentes de tratamento, entende-se ser fundamental não só a realização de uma análise de impacto regulatório, conforme já previsto no § 3º do art. 55-J, XXIV, da LGPD, mas também de um juízo de proporcionalidade, guiando-se pelos critérios de adequação, necessidade e proporcionalidade em sentido estrito, de modo a verificar, respectivamente, se determinada medida proposta é adequada e necessária para o atingimento do fim proposto, se o objetivo não pode ser promovido de outra maneira com menores riscos à livre concorrência e de criar assimetrias, bem como se os motivos que a fundamentam têm o peso suficiente para justificá-la.

16. Feitas estas considerações preliminares, a ABIPAG apresenta a seguir, em formulário próprio anexo, suas contribuições às questões propostas pela ANPD, com o intuito de colaborar para o aprimoramento do ambiente regulatório no País.

17. Sendo o que servia para o momento, a ABIPAG agradece mais uma vez a oportunidade de se manifestar, reforçando seu compromisso com a promoção da livre concorrência, livre iniciativa e isonomia do mercado, e coloca-se à disposição para quaisquer esclarecimentos e informações adicionais que se façam necessários.

Atenciosamente,

_____

ABIPAG – ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS - ABIPAG

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	A ABIPAG acredita que será um desafio para a ANPD a edição de normas, orientações e procedimentos simplificados e diferenciados para agentes de tratamento de dados de pequeno porte que não criem barreiras para a configuração de novos negócios. Como se sabe, as *startups* têm como características intrínsecas ao seu modelo de negócio condições de extrema incerteza e, especialmente no estágio de desenvolvimento, enorme dificuldade para financiar os seus projetos, por conta da ausência de garantias e geração de caixa. Portanto, é fundamental que a ANPD considere tais limitações e peculiaridades para que os custos de conformidade com a LGPD e o risco regulatório, em conjunto com o próprio risco inerente ao modelo de negócio, não prejudique iniciativas desta natureza. Isto porque, ao imputar, logo na partida, o ônus de estruturar novos negócios considerando todas as complexidades da Lei, pode-se acabar por desincentivar o desenvolvimento de novos serviços. Nessa linha, como destacado em suas notas introdutórias, a ABIPAG considera que o desafio regulatório colocado perante a ANPD é encontrar a justa medida, i.e., uma opção proporcional, que assegure grau de proteção dos titulares de dados, sem, no entanto, erguer barreiras regulatórias que inviabilizem a diversificação da atividade econômica. Nesse sentido, importante que a regulação da ANPD tenha como foco negócios que representam grande risco aos seus usuários, uma vez que tratam grande volume de dados e que, por terem elevado poder econômico, têm condições de garantir que todos os mecanismos necessários à proteção aos direitos dos titulares de dados

	sejam respeitados e de arcar com ônus regulatório proporcional ao risco que representam. Além disso, para promover a isonomia entre agentes dominantes e os destinatários da regulação que motiva a presente Tomada de Subsídios, é necessário que sejam criadas ferramentas que garantam que esses agentes não tenham o domínio exclusivo sobre os dados que tratam. Chama-se atenção para as grandes empresas de tecnologia, as BigTechs, que, além de terem protagonizado incidentes relevantes no tratamento de dados, têm poder de mercado suficiente para utilizá-los como forma de restringir a concorrência. Com isso, ferramentas adequadas para viabilizar, por exemplo, o open data e a interoperabilidade devem ser estabelecidas, a fim de permitir que agentes entrantes tenham condições de acessar esses mercados e concorrer com agentes incumbentes, enquanto protege-se o direito fundamental dos titulares à proteção de seus dados pessoais.
Existem sugestões para endereçamento do problema?	A ABIPAG entende que, em um primeiro momento, poderia ser cogitada uma espécie de flexibilização para micro e pequenos negócios, e *start-ups*, estabelecendo-se apenas obrigações de resultado (e.g.. observância dos direitos dos titulares), sem, no entanto, disciplinar os meios para o atingimento destes resultados. Sob o ponto de vista da ANPD, isto oportunizaria uma melhor absorção das particularidades dos agentes de pequeno porte, além de garantir maior período para adaptação e promoção das regras a eles aplicáveis. Ao mesmo tempo, viabilizaria que as empresas enquadradas nesta categoria otimizassem seus procedimentos internos de forma mais adequada, sem que isso prejudicasse o exercício de direitos dos titulares. Nessa linha, a ANPD deveria se preocupar em privilegiar uma abordagem responsiva e educativa quanto a tais negócios, concentrando esforços na edição de *soft laws,* a exemplo de guias de boas-práticas e manuais, bem como na resposta a consultas, que serviriam de balizas para estruturação de procedimentos internos visando a dar cumprimento às determinações legais. Caso, em análises concretas, se constate a insuficiência destes procedimentos para o atingimento dos resultados determinados na Lei, caberia, então, à ANPD, quando provocada, chamar o agente econômico / controlador do tratamento para com ela transacionar, tomando compromissos específicos visando ao aperfeiçoamento dos procedimentos internos em matéria de proteção de dados, antes que se proceda a qualquer tipo de apenamento.

	Além destas recomendações preliminares, a ABIPAG sugere à ANPD, quando da regulamentação aplicável aos agentes de pequeno porte, a adoção das seguintes medidas: • **Alinhamento da regulamentação com as políticas públicas de incentivo aos novos negócios, à criação de um ambiente mais favorável à inovação e à ampliação da competição** que já vêm sendo adotadas no Brasil, inclusive, mas não se limitando, àquelas desenvolvidas pelo Banco Central do Brasil (e.g., Open Banking, PIX). • Em homenagem à previsibilidade, **estipulação de critérios específicos, transparentes e proporcionais para aplicação de sanção aos entes de pequeno porte**, as quais somente devem ser aplicadas em *ultima ratio*, uma vez que a aplicação de multas ou obrigações pode comprometer a saúde financeira de tais empresas, por serem notadamente mais vulneráveis. • **Dispensa da obrigação de elaboração / manutenção de DPIAs**, que poderia ser determinada pela ANPD à vista de casos concretos, quando provocada, circunstância em que caberia ao controlador demonstrar a legitimidade do tratamento por ele realizado. Subsidiariamente, sugere-se, ao menos, a mitigação desta obrigação em relação aos agentes de pequeno porte, dispensando-os ou reduzindo a quantidade de informações necessárias, uma vez que o nível de detalhamento pode representar um óbice ou barreira a estes. • **Dispensa de cumprimento da obrigação de indicação de um Encarregado pelo Tratamento de Dados Pessoais ou estipulação de critérios de inexigibilidade**, como a reduzida quantidade de funcionários, desde que o tratamento de dados não seja o *core business* da empresa. Esta dispensa poderia estar vinculada, por exemplo, à realização de cursos que promovam o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança e/ou que a função seja executada por um setor já existente da companhia (e.g., Jurídico, TI).

	• **Estipulação de limitações operacionais e/ou temporais quanto às requisições dos titulares de dados a agentes de tratamento de pequeno porte**, de forma a atenuar potencial abuso do exercício de direitos, como: (i) restrição de solicitação de dados sob forma impressa e por outros meios que não o canal oficial disponibilizado pela empresa, uma vez que demandaria recursos financeiros e humanos, tão escassos a grande parte delas, especialmente por conta do estado de calamidade pública que se instalou no País em razão da pandemia do coronavírus (COVID-19); (ii) vedação a solicitações coletivas e/ou feitas por terceiros, que não o próprio titular; (iii) restrição temporal para pedidos gratuitos pelo mesmo titular; e (iv) dilação do prazo de resposta de 15 para 30 dias, contados da data da conclusão do processo de identificação/autenticação do titular, diante da potencial dificuldade operacional e impossibilidade de automatização de processos para atendimento de demandas desta natureza. • **Dispensa da obrigação de manutenção de registros contínuos de operações de tratamento de dados**, na forma de flexibilização regulatória, nos estágios iniciais de novos negócios e que, gradualmente, seja estabelecida a obrigação de registros apenas daquelas atividades relacionadas ao *core business* do agente econômico, ou que possam representar risco ao titular dos dados. • **Manutenção da dispensa da revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses dos titulares ser feita por pessoa natural**, tendo em vista que, conforme mencionado na Mensagem de Veto nº 288/2019, "tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras [...]"[2]. • **Estabelecimento de regras simplificadas e diferenciadas sobre o direito de portabilidade de dados para agentes de tratamento de dados pessoais de pequeno porte**. Neste sentido, sugere-se a adoção das seguintes medidas: (i) determinação de que o atendimento deste direito se dará pela mera disponibilização, em formato legível e de fácil acesso, das informações do titular de modo estruturado;

[2] Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm.

	(ii) não imposição de qualquer obrigação relacionada à implantação de sistemas *standard* / padrão, tendo em vista as grandes peculiaridades existentes entre cada setor econômico e a inviabilidade de exigência de capacidade computacional / tecnológica a esta categoria de empresas; e (iii) indicação expressa de que os procedimentos internos sobre portabilidade adotados por cada empresa devem ser protegidos pelo segredo comercial.
Quais são as oportunidades relacionadas ao tema?	A ABIPAG não possui comentários adicionais a fazer.
Quais são as experiências internacionais sobre o tema?	O GDPR prevê que empresas com menos de 250 funcionários estão desobrigadas de registrar suas operações de tratamento de dados pessoais, a menos que tal tratamento tenha potencial de gerar riscos para os direitos e liberdades dos titulares dos dados, não seja ocasional ou inclua determinadas categorias especiais de dados[3]. Além disso, a indicação de um *Data Protection Officer* (DPO) somente é necessária em determinadas situações previstas na Lei. Apesar de não estabelecer qualquer regime diferenciado no que se referem às demais obrigações, o Regulamento Europeu explicitamente incentiva as instituições e órgãos da União Europeia, os Estados-Membro e suas respectivas autoridades supervisoras a considerarem as necessidades específicas das micro, pequenas e médias empresas em seus regulamentos, devendo a noção da definição destas categorias de empresas se basear na *Commission Recomendation No. 2003/361/EC*[4]. Por conseguinte, tal instrumento define média empresa como aquela que possui menos de 250 funcionários e cujo volume de negócios não excede € 50 milhões ou cujo balanço total anual não excede € 43 milhões; pequena empresa como aquela que possui menos de 50 funcionários e cujo volume de negócios ou balanço total anual não excedem € 10 milhões;

[3] Neste sentido, veja-se *position paper* sobre a dispensa de cumprimento da obrigação de manutenção de registros das atividades de tratamento de dados, elaborado pelo *Article 29 Working Party* e endossado pelo *European Data Protection Board* (EDPB): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.
[4] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

	e microempresa como aquela que possui menos de 10 funcionários e cujo volume de negócios ou balanço total anual não excedem € 2 milhões. Além disso, o GDPR determina que os Estados-Membros, autoridades supervisoras, o Conselho e a Comissão Europeia incentivem a criação de mecanismos de certificação, selos e marcas de proteção de dados, os quais devem levar em consideração as necessidades e características específicas das micro, pequenas e médias empresas, a fim de viabilizar a demonstração do cumprimento de referido regulamento pelos controladores e operadores de maneira prática à empresas, indivíduos e órgãos reguladores. Outra norma que pode ser destacada é a *California Consumer Privacy Act* (CCPA), que assegura um leque de direitos relacionados à privacidade dos consumidores da Califórnia. Por expressa previsão legal, o CCPA só se aplica a empresas que têm uma receita anual bruta de mais de US$ 25 milhões, derivam mais de 50% de sua receita anual da venda de dados pessoais, ou compram, vendem ou compartilham dados pessoais de mais de 50.000 consumidores por ano. De modo diverso, a lei australiana de proteção de dados pessoais (*Privacy Act 1988*)[5] optou por declarar que a as pequenas empresas estão isentas de cumprir com as obrigações nela previstas, com exceção daquelas empresas que exercem determinadas atividades estabelecidas em rol taxativo (e.g., fornecedores de serviços de saúde, *bureaus* de crédito, empresas que compram e/ou vendem dados pessoais para qualquer benefício, serviço ou vantagem, empresas que optam por serem obrigadas a cumprir a Lei, etc.). Nos termos desta Lei, pequena empresa é – excluídas as exceções – toda aquela que, no ano fiscal anterior, teve faturamento anual menor ou igual a U$ 3 milhões.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	De fato, não há unanimidade sobre a estipulação de critérios para definição de microempresas, empresas de pequeno porte e *startups*. Na prática, observa-se na legislação específica (e.g., Lei nº 9.841/1999, Lei Complementar nº 123/2006) e nas regulamentações e diretrizes adotadas pelos órgãos governamentais e instituições financeiras (e.g., SEBRAE, BNDES, IBGE, RFB) uma diversidade de métodos para definição destas categorias de empresas previstos, como o valor do faturamento, o número de funcionários etc. Em verdade, a

[5] Disponível em: https://www.legislation.gov.au/Details/C2021C00024.

	utilização de conceitos díspares decorre do fato de a finalidade e os objetivos promovidos por estes entes são distintos (e.g., tributação, disponibilização de crédito, regulamentação, realização de estudos e pesquisas). No contexto da LGPD, destaca-se que classificar estes agentes de pequeno porte por número de funcionários é ineficaz, pois acaba por desconsiderar diversos fatores, como o *core business* das empresas, o volume de dados pessoais tratados e de negócios e o próprio faturamento. De modo similar, a ABIPAG entende que a mera aferição do faturamento não é suficiente para caracterizar agentes econômicos de pequeno porte para fins de implementação das obrigações da LPGD. Desse modo, considera-se necessário o estabelecimento de critérios adicionais em regulamento específico, que dialoguem com as finalidades e objetivos perseguidos pela ANPD e com os princípios e peculiaridades da legislação de proteção de dados pessoais Neste caso, a ABIPAG sugere que a definição de agentes de tratamento de dados de pequeno porte seja feita considerando aspectos como a estrutura, a escala e o volume de suas operações (incluindo o número de clientes), natureza do serviço prestados, a sensibilidade dos dados tratados, a probabilidade e gravidade dos danos para os titulares, o prazo de constituição e o número de funcionários da empresa. Especificamente em relação a *startups* ou empresas de inovação, vale destacar que tramita no Congresso Nacional o PLP nº 146/2019, que busca estabelecer mecanismos de incentivo ao empreendedorismo inovador e, portanto, pode servir como norte para a ANPD. Uma das maiores contribuições desta iniciativa é justamente a definição de critérios objetivos (e.g., tamanho e idade da empresa) e subjetivos (e.g., autodeclaração) para identificá-las, de modo a complementar aquelas definições presentes na legislação em vigor, em especial a Lei Complementar nº 123/2006, mencionada na Nota Técnica nº 1/2021/CGN/ADPD. De todo o modo, a ABIPAG entende que os critérios para flexibilização das obrigações legais não podem ser exaustivos, devendo-se prever mecanismos que possibilitem a habilitação, no regime flexível, de agentes econômicos não tipificados nas hipóteses regulamentares. Tal habilitação, por certo, dependeria de prévia aprovação da ANPD, após análise do caso concreto e das justificativas apresentadas pelo requerente.

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)?	De um modo geral, a União Europeia tem atuado de modo responsivo, restringindo-se à simplificação de determinadas obrigações, estabelecimento de diretrizes, recomendações e melhores práticas, além da promoção do GDPR. Sob este tema, faz-se referência aos comentários realizados na questão sobre experiências internacionais.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	A ABIPAG acredita que a maior dificuldade dos agentes de pequeno porte em relação a este tema está nos custos e no prazo para levantamento e registro de todas as operações de tratamentos de dados pessoais por eles realizados. Isto porque, como se sabe, os procedimentos internos em tais empresas estão em formação e o prazo para a solução de demandas acaba sendo mais extenso se comparado às demais empresas. Neste sentido, como medida de flexibilização, sugere-se (i) a dispensa da obrigação de manutenção de registros contínuos de operações de tratamento de dados, nos estágios iniciais de novos negócios e que, (ii) gradualmente, seja estabelecida a obrigação de registros apenas daquelas atividades relacionadas ao *core business* do agente econômico, o que possam representar risco ao titular dos dados.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Grande parte dos agentes de tratamento de dados de pequeno porte não possuem recursos para contratação de um funcionário e/ou assessoria especializada para o exercício da função de encarregado de dados. Portanto, a ABIPAG sugere que tais agentes, a serem identificados conforme os critérios mencionados anteriormente, sejam dispensados do cumprimento de tal obrigação ou, subsidiariamente, que a ANPD estipule critérios de inexigibilidade, como a reduzida quantidade de funcionários, desde que o tratamento de dados não seja o *core business* da empresa. Em qualquer caso, a ABIPAG entende ser primordial que a ANPD expressamente autorize a cumulação do cargo de Encarregado com outros de funções similares, de forma a alinhar sua regulamentação com a dos demais órgãos reguladores (e.g., p. único, art. 32 da Resolução Conjunta CVM-BCB nº 1/2020, relacionada à obrigação de designar diretor responsável pelo compartilhamento de dados e serviços e a possibilidade do mesmo desempenhar outras funções) e não elevar os riscos e ônus regulatórios de forma desproporcional e/ou criar barreiras desnecessárias.

Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	A ABIPAG entende que, com relação a agentes de pequeno porte, a ANPD deveria prestigiar uma abordagem de resultado ao invés de fixar obrigações de meio. Neste sentido, desde que observados os parâmetros fixados em Lei para que se tenham tratamentos legítimos de dados pessoais, deveria ser dispensadas formalidades capazes de incrementar o custo da operação comercial, a exemplo da elaboração prévia de Relatórios de Impacto de Proteção de Dados (DPIA). Na avaliação da ABIPAG, constatada a existência de um legítimo interesse e /ou de situações que comportem risco para o titular, caberia ao controlador que se caracterize como agente de pequeno porte adotar as cautelas necessárias para dar cumprimento às finalidades da Lei. E nessa linha, a obrigação de elaboração / manutenção de DPIAs poderia ser determinada pela ANPD à vista de casos concretos, quando provocada, circunstância em que caberia ao controlador demonstrar a legitimidade do tratamento por ele realizado. Subsidiariamente, sugere-se ao menos a mitigação da obrigação de elaboração destes relatórios para agentes de pequeno porte, para que seja reduza a quantidade de informações necessárias, uma vez que o nível de detalhamento pode representar um óbice ou barreira a estes *players*.
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?	A ABIPAG acredita que a maior dificuldade dos agentes de pequeno porte em relação a este tema está no prazo para adequação à LGPD e no cumprimento das obrigações de meio. Como se sabe, os procedimentos internos em tais empresas estão sob definição, de maneira que o atendimento da Lei, em todos seus pormenores (incluindo prazo para a solução de demandas) acaba sendo mais extenso e custoso se comparado às demais empresas. Sugere-se, neste sentido, que a ANPD estabeleça, com relação a agentes de pequeno porte, obrigações de resultado, sem, no entanto, detalhar procedimentos a serem adotados (ao contrário, deveriam ser adotados mecanismos de *soft laws / guidelines* para guiar a estruturação de procedimentos internos). Uma vez amadurecido o negócio e atingidas as condições para atendimento integral das obrigações legais e regulamentares, caberia, então, prever um cronograma para implementação gradual de tais procedimentos, franqueando-se a oportunidade de que planos de adequação sejam levados ao prévio conhecimento da

	Autoridade, que poderia, diante de circunstâncias concretas, estabelecer prazos maiores, se assim necessário. Além disso, no que se refere à aplicação de sanção, as quais somente devem ser aplicadas em *ultima ratio*, sugere-se que a ANPD estipule critérios específicos (previamente determinados), transparentes e proporcionais aos entes de pequeno porte, uma vez que a aplicação de multas ou obrigações pode comprometer a saúde financeira de tais empresas, por serem notadamente mais vulneráveis.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	A ABIPAG entende que a principal dificuldade dos agentes de pequeno porte está relacionada à ausência de padrões estabelecidos pela ANPD e pelo tema ainda não ter sido plenamente regulamentado, o que acaba por gerar um ambiente de insegurança jurídica, dificultando a formalização de uma política que esteja em *compliance* com a legislação aplicável. De todas as formas, em linha com seus comentários anteriores, a ABIPAG considera que, com relação a agentes de pequeno porte, deve a ANPD prestigiar obrigações de resultado, sem especificar meios para tanto.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Idem à resposta anterior.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	Idem à resposta anterior.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Na linha destacada em seus comentários acima, a ABIPAG entende que a definição e detalhamento de padrões a serem adotados em certos negócios tem o potencial de incrementar custos de operação. Diante disso, a ABIPAG considera que a obrigação de portabilidade deve ser finalística, sem que sejam estabelecidos formatos, tecnologias etc. para que tal portabilidade seja operacionalizada.

	Considerando isto, sugere-se o estabelecimento de regras simplificadas e diferenciadas sobre o direito de portabilidade de dados para agentes de tratamento de dados pessoais de pequeno porte, mediante a adoção das seguintes medidas: (i) determinação de que o atendimento deste direito se dará pela mera disponibilização, em formato legível e de fácil acesso, das informações do titular de modo estruturado; (ii) não imposição de qualquer obrigação relacionada à implantação de sistemas *standard* / padrão, tendo em vista as grandes peculiaridades existentes entre cada setor econômico e a inviabilidade de exigência de capacidade computacional / tecnológica a esta categoria de empresas; e (iii) indicação expressa de que os procedimentos internos sobre portabilidade adotados por cada empresa devem ser protegidos pelo segredo comercial. Vale destacar que a regulamentação da portabilidade de dados se torna mais premente e relevante à medida que o número de clientes da empresa aumenta, razão pela qual sugere-se que, nesse momento, todos os esforços necessários sejam envidados em prol da adoção de mecanismos que assegurem a portabilidade de dados no âmbito de grandes plataformas digitais (e.g., redes sociais, plataformas de mobilidade etc.).
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	A ABIPAG acredita que é primordial a busca por um instrumento regulatório que promova um equilíbrio entre a proteção dos direitos dos titulares de dados e da competitividade, inovação e liberdade como uma garantia no exercício de atividades econômicas, permitindo um funcionamento mais eficiente do mercado e o surgimento de novos modelos de negócios que contribuam para a diversificação dos serviços prestados, o que está em linha, aliás, com os comandos da Lei nº 13.874/2019, que instituiu a Declaração de Direitos de Liberdade Econômica. Nessa linha, a ABIPAG considera que a ANPD deve prestigiar, com relação a agentes de pequeno porte, a adoção de mecanismos de *soft law*, incluindo manuais e guias de boas práticas.
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

***

Tomada de Subsídios 1/2021 - Contribuições ABERT

Rodolfo Salema [redacted]

seg 01/03/2021 21:05

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

[redacted]

2 anexos

Abert - Contribuicoes PME - Modelo ANPD. vf.docx; Abert - Contribuicoes PME - Modelo ANPD. vf.pdf;

Prezados, boa noite.

Encaminhamos em anexo as **contribuições da ABERT (Associação Brasileira de Emissoras de Rádio e Televisão)**, com relação à tomada de subsídios 1/2021 sobre a regulamentação da aplicação da Lei nº 13.709/2018 para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação (disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/ainda-na-semana-internacional-da-protecao-de-dados-anpd-inicia-tomada-de-subsidios-sobre-microempresa).

Em tempo, solicitamos, se possível, reunião com a Coordenação-Geral de Normatização da ANPD para endereçamento de alguns pontos da contribuição relativos ao setor de rádio e televisão, colocando-nos à disposição para eventuais esclarecimentos.

Favor confirmar o recebimento do e-mail.

Att.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Associação Brasileira de Emissoras de Rádio e Televisão (“ABERT”)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	O Brasil possui em torno de 19 milhões de empresas em seu território, de acordo com dados do DataSebrae[1]. Destas, cerca de 17 milhões pertencem às categorias de Empresa de Pequeno Porte (EPP), Microempresa (ME) e Microempresa Individual (MEI). São números que revelam uma realidade brasileira: as pequenas empresas representam um dos motores da nossa economia, sendo responsáveis por levar emprego e renda para grande parte dos lares do país. Para além das dificuldades habituais associadas ao chamado "Custo Brasil", as pequenas empresas também acabaram sendo as mais duramente afetadas pela grave crise econômica decorrente da pandemia de Covid-19. Não é exagero, portanto, afirmar que cada recurso de uma pequena empresa é fundamental para sua sobrevivência.

[1] SEBRAE. Painel de empresas. Disponível em: <https://datasebrae.com.br/totaldeempresas/>.

	Essa realidade não é diferente no setor de radiodifusão. Conforme pesquisa realizada pela Confederação Nacional da Comunicação Social (CNCOM), a maioria[2] das emissoras de rádio e televisão do país atendem pelo regime de tributação do Simples Nacional - o qual tem como limite de faturamento R$4.800.000,00 por ano. A necessidade de adequação das empresas brasileiras à nova realidade da LGPD pode acabar penalizando sobremaneira os pequenos negócios, principalmente no momento econômico delicado pelo qual passa o país. Afinal, o processo de adequação à nova legislação está associado a consideráveis custos. Estimativas dão conta de que a adequação tem custo que varia de R$ 50 mil a R$ 800 mil, a depender do segmento econômico[3]. Dentre as medidas necessárias de adequação à nova norma, a manutenção do registro de operações de tratamento de dados pessoais, a contratação de profissionais específicos para lidar com essa tarefa, bem como a possibilidade de sujeição às multas administrativas, que podem chegar a 2% do faturamento, constituem uma série de novos encargos, que pode efetivamente inviabilizar a operação de muitas pequenas empresas do Brasil. Para as startups brasileiras, que em muitos casos lideram modelos de negócio inovadores e disruptivos, tão importantes para o bem-estar do consumidor e também para o desenvolvimento tecnológico nacional, as imposições regulatórias da LGPD podem acabar funcionando como verdadeiras barreiras à entrada, limitando seu crescimento. Por tudo isso, a previsão constante do art. 55-J, XVIII, da LGPD mostra sensibilidade importante do legislador quanto à necessidade de equacionar o direito de proteção dos dados pessoais e as garantias previstas na LGPD com o porte dos agentes econômicos, a inovação e o desenvolvimento econômico. Que a ANPD tenha escolhido esse ponto como prioridade na sua agenda regulatória e o selecionado para sua primeira Tomada de Subsídios também é sinalização importante da Autoridade, no sentido de que está atenta à realidade do país, da economia e deseja cooperar com o mercado.

[2] Mais especificamente, a pesquisa demonstra que **54% das empresas estão no regime do Simples, no caso de TV aberta, e 66.79%, no caso de Rádio**.
[3] O cálculo é de Edgar D'Andrea, sócio da PwC Brasil, conforma matéria do Valor Econômico. Disponível em: <https://valor.globo.com/publicacoes/suplementos/noticia/2020/08/21/custo-da-conformidade-pode-variar-de-r-50-mil-a-r-800-mil.ghtml>.

	No âmbito da radiodifusão, é importante destacar que o curso tradicional dos negócios dessas empresas de pequeno porte, na prática, é pouco intensivo em tratamentos de dados pessoais, já que boa parte do trabalho consiste em produção de conteúdo artístico ou jornalístico, os quais sabidamente estão foram do alcance da lei. Além disso, a relação com o público-alvo de seus produtos, ouvintes ou telespectadores não envolve usualmente o tratamento dos dados pessoais destes de forma intensiva ou com viés de consumo. Não obstante, a dificuldade mais substancial e de maior impacto nas pequenas emissoras de radiodifusão é o custo para arcar com a instalação e manutenção de sistemas de segurança de dados, aparelhos necessários e a contratação de equipes especializadas para essa atividade, que demandarão recursos muito além da capacidade e porte de pequenos agentes do setor. A eventual necessidade de se apontar um encarregado e o temor de multas administrativas futuras também foram identificadas como preocupações do setor. Além disso, a operacionalização de mecanismos para a obtenção de consentimento dos titulares será complexa, já que muitas emissoras estão habituadas a captar informações pessoais sem seguir os padrões adotados na lei (até por conta da finalidade), que são bastante exigentes. Nesse contexto, a Abert entende que a mudança de cultura tem o potencial de ser traumática e gerar resistência do setor se não for conduzida com parcimônia, de modo que uma compreensão da Autoridade sobre as dificuldades se faz essencial para o próprio sucesso do processo de consolidação da política nacional de proteção de dados no país.
Existem sugestões para endereçamento do problema?	Primeiramente, estabelecer regimes diferenciados de aplicação da LGPD para agentes de pequeno porte seria um caminho salutar, o que é fundamental para isentar os pequenos negócios de encargos excessivos e conferir maior segurança jurídica para o mercado. O estabelecimento de regimes diferenciados para agentes de pequeno porte é obrigação constitucional da União, de modo que se observam diversas iniciativas de desburocratização e regimes tributários especiais que visam promover o empreendedorismo e inovação no país a partir destes agentes (ex: Lei da Liberdade Econômica). Em face dos custos e dificuldades associadas à implementação da LGPD, nota-se oportunidade de adoção de regime especial para agentes de pequeno porte, com a isenção de algumas normas e obrigações, sem que estas gerem efeitos deletérios para os direitos dos titulares de dados pessoais.

	Também a atuação orientativa por parte da ANPD, com a confecção de guias de instruções, criação de websites interativos e canais de atendimento, além do oferecimento de formulários para a adequação, seriam medidas importantes para auxiliar as atividades de adequação de pequenos empresários, estimulando o desenvolvimento de uma cultura de proteção de dados entre os pequenos negócios. Ainda, como será mais bem desenvolvido na última questão, a adoção de *sandboxes* regulatórios com flexibilização de normas em espaços controlados seria uma medida interessante para fomentar a inovação entre essas empresas e assegurar que suas iniciativas comerciais inovadoras estejam em conformidade com a legislação de proteção de dados pessoais.
Quais são as oportunidades relacionadas ao tema?	Ao se propor a regulamentar o tema, a ANPD tem a oportunidade de desenvolver um padrão regulatório mais equalizado para agentes econômicos de pequeno porte, que passarão assim a contar com uma regulação mais adequada aos riscos envolvendo as suas atividades e estariam isentos de encargos excessivos e desnecessários num momento em que a economia brasileira padece de grave crise. Também é a oportunidade de, através de uma regulação apropriada, difundir a tão desejada e necessária cultura de proteção de dados pessoais no Brasil, que através de um desenho institucional adequado pode chegar aos pequenos agentes econômicos, muitas vezes sem qualquer familiaridade com o assunto. Igualmente, trata-se de chance de estabelecer um arcabouço regulatório pensado para o fomento da inovação, uma vez que reduz o encargo regulatório para agentes interessados em desenvolver modelos de negócio disruptivos ou, até mesmo, de agentes que passam por reformulação em seus modelos. Mais, representa oportunidade de promover instrumentos regulatórios ainda jovens e pouco difundidos na realidade regulatória brasileira.
Quais são as experiências internacionais sobre o tema?	A preocupação com busca de um equilíbrio entre a proteção de dados e as peculiaridades envolvidas na situação de pequenas empresas vem sendo observada nas experiências internacionais de outras jurisdições que contam com um arcabouço regulatório para proteção de dados consolidado.

	Na União Europeia (UE), que possui o normativo de proteção de dados referência para todo o mundo (o *General Data Protection Regulation* - GDPR), as empresas com até 250 funcionários estão isentas de manter os registros de atividades de tratamento de dados, de acordo com o art. 30 (5) do GDPR, ressalvadas oportunidades em que o tratamento: (i) pode resultar em risco aos direitos e liberdades de titulares de dados pessoais, (ii) é realizado de forma não ocasional ou (iii) envolve dados pessoais sensíveis. O GDPR também estabelece, em seu art. 37, que estão desobrigadas de apontar um Data Protection Officer (figura equivalente ao Encarregado pelo Tratamento de Dados Pessoais, na LGPD) as empresas que não tenham como atividade principal o processamento de dados em larga escala, hipótese que tem o potencial de beneficiar pequenos negócios. Vale destacar que a definição de "larga escala" no regramento europeu é um ponto que provoca debates e insegurança jurídica nos agentes econômicos, tendo em vista que o GDPR não estabelece qualquer definição mais precisa nesse sentido. O *Article 29 Working Party*, órgão da Comissão Europeia responsável pela interpretação de normas de proteção de dados pessoais na UE até meados de 2018 e sucedido pelo European Data Protection Board, chegou a analisar esses dispositivos do GDPR[4]. Entretanto, trouxe uma interpretação bastante ampla do que poderia ser essa larga escala, criando cenário de incerteza entre as organizações. Conforme será detalhado, a criação de critérios claros e objetivos sobre a incidência do regime especial é relevante pois sua ausência pode criar incentivos perversos para que agentes deixem de se adequar, quando necessário, ou acabem sendo obrigados a implementar a legislação como um todo, independentemente dos regimes especiais, por receio de eventuais sanções. Por se tratar da legislação consolidada, a experiência europeia é rica em exemplos práticos, e nesse sentido, uma pesquisa realizada pelo GDPR.EU em maio de 2019[5], por ocasião do 1 ano da entrada em vigor do GDPR, mapeou como estava o *compliance* de proteção de dados das pequenas empresas europeias. Embora a imensa maioria dos entrevistados (donos de pequenos negócios em Espanha, Reino Unido, França e Irlanda) tenha respondido que acreditavam estar adequados ao GDPR e cientes de sua importância, aproximadamente metade dos entrevistados desconhecia conceitos básicos da legislação e estava falhando em cumprir requisitos básicos do tratamento de dados.

[4] ARTICLE 29 DATA PROTECTION WORKING PARTY. POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR. Disponível em: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045>; ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Officers. Disponível em: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

[5] 2019 GDPR Small Business Survey. Disponível em: <https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf>.

	Nos EUA, o principal marco legal de proteção de dados e privacidade é o *California Consumer Privacy Act* (CCPA), lei do estado da California que vem sendo tomada como referência para diversas empresas elaborarem suas políticas de privacidade naquela jurisdição. O CCPA define como empresas sujeitas à sua aplicação, na Seção 1798.140, apenas aquelas que (i) apresentam faturamento anual superior a 25 milhões de dólares; (ii) que sozinhas ou em conjunto comprem, recebam, vendam ou compartilhem informações pessoais de 50 mil consumidores da California anualmente; e (iii) obtenham 50% ou mais do seu faturamento anual a partir da venda de dados pessoais. Contudo, a definição dada pelo CCPA a "informações pessoais" é tão ampla que, na prática, quase qualquer empresa de tecnologia, independentemente de seu tamanho, estaria contemplada. Por exemplo, agentes atuando sob o regime do CCPA indicam que empresa cujo site receba apenas 137 visitantes por dia, por exemplo, já está sujeita às obrigações do CCPA[6]. Na Austrália, a maior parte dos pequenos negócios não está sujeita à legislação de proteção de dados do país. Empresas com um faturamento anual inferior a 3 milhões de dólares estão desobrigadas de se adequar, exceto quando suas atividades se encaixarem num rol qualitativo[7] que inclui serviços de saúde, proteção ao crédito, entre outros. Partindo para a América Latina, na Colômbia, estão isentas do Registro Nacional de Bases de Dados as pequenas sociedades cujos ativos não ultrapassem a cifra de 3.630.800.000 de pesos colombianos (algo em torno de 5,5 milhões de reais, pela cotação atual do peso), bem como as organizações sem fins lucrativos. Na Argentina, em que pese o atual framework regulatório não estabelecer qualquer diferenciação para pequenas empresas, tramita desde 2018 um projeto de lei bastante parecido com o GDPR, em que estariam isentas de apontar um DPO as empresas que não realizem tratamento de dados em grande escala, exatamente como diz o regramento europeu. No caso de startups, mais especificamente, uma experiência internacional interessante vem do Reino Unido, onde a autoridade de proteção de dados local, a *Information Commissioner's Office* (ICO) delineou um modelo de *sandbox* regulatória para situações de tratamento de dados

[6] NATIONAL LAW REVIEW. What Startups should know about the California Consumer Privacy Act. Disponível em: <https://bit.ly/2M65SKg>.
[7] AUTRALIAN GOVERNMENT. Privacy for organisations: Small business. Disponível em: <https://www.oaic.gov.au/privacy/privacy-for-organisations/trading-in-personal-information/>.

	pessoais[8]. Ainda em fase de testes, o modelo visa fornecer suporte para empresas e organizações que utilizam dados pessoais no desenvolvimento de produtos e serviços genuinamente inovadores, com claros benefícios para o público. As empresas participantes podem, dessa forma, dar prosseguimento a seus processos inovativos e incorporar um arcabouço de proteção de dados sob o olhar vigilante da Autoridade.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Primeiramente, cumpre pontuar que no Brasil, os conceitos de microempresas e empresas de pequeno porte já estão estabelecidos pelo art. 3º da Lei Complementar nº 123/2006, e levam em conta a receita bruta anual para a classificação do porte dos empreendimentos. De forma semelhante, o Banco Nacional do Desenvolvimento (BNDES) emprega esta definição legal para a classificação do porte de seus clientes.[9] O IBGE, por sua vez, utiliza definição de porte de empresa a partir do número de funcionários. Para a Indústria, por exemplo, o IBGE considera microempresas aquelas com até 19 empregados e empresas de pequeno porte aquelas que contam com 20 a 99 empregados. No âmbito de atuação da Abert, nossos associados também entendem que a concepção de pequeno porte está associada a outros aspectos, devendo ir além da delimitação estabelecida a partir do faturamento. As emissoras poderiam ser classificadas conforme número de funcionários e escala de dados que tratam, considerando-se a natureza, o âmbito e a finalidade, se o tratamento é em larga escala, bem como se é feito de forma regular e sistemática. Neste sentido, a proposta de normativo ora apresentada conta com dois critérios complementares para a definição dos agentes afetados pelo regime especial. Entende-se que, ainda que critérios quantitativos tenham sua relevância por serem diretamente aplicáveis, é necessário adotar um critério qualitativo a partir das atividades exercidas pelos agentes de tratamento de dados pessoais, para que mesmo que empresas que não se encaixem no critério quantitativo possam ser eximidas da aplicação de regras da LGPD em razão de atividades que não gerem impactos relevantes para os titulares de dados pessoais. Nesse sentido, é importante que essas definições qualitativas conversem com parâmetros da própria LGPD, como a definição de dados sensíveis, o escopo dos titulares de dados afetados, entre outros.

[8] REINO UNIDO. Information Commissioner's Office. The Guide to Sandbox. Disponível em: <https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/>.
[9] BNDES. Porte de Empresa. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/financiamento/guia/porte-de-empresa.

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)?	Além das já citadas regras de isenção prescritas no GDPR para pequenas empresas, a principal atuação das autoridades da União Europeia (UE) no sentido de auxiliar que agentes de pequeno porte estejam em conformidade com a legislação, se dá através da função educativa, com orientações específicas para micro e pequenas empresas, emitidas tanto pelas Autoridades de Proteção de Dados a nível continental, quanto pelas dos Estados-membros. No âmbito da UE, a Agência Europeia de Cibersegurança (ENISA), responsável por auxiliar na prevenção de problemas de Segurança da Informação entre as Instituições do Bloco, frequentemente emite Guias com orientações, alguns dos quais são especificamente direcionados para pequenas empresas. Já foram publicados Guias sobre Segurança da Computação em Nuvem e sobre Segurança do Processamento de Dados, especificamente para pequenos negócios[10]. Além disso, a Comissão Europeia conta com um website exclusivamente dedicado a esclarecer a aplicação do GDPR para pequenas empresas[11], elaborado sob a forma de infográfico e com indicações bastante didáticas do passo a passo para que esses negócios se adequem à legislação. Adentrando as jurisdições dos Estados-membros do Bloco, uma pesquisa realizada em 2020, com financiamento da UE[12], concluiu que pouco menos de um terço das autoridades de proteção de dados europeias oferecem orientações direcionadas especificamente para empresas de pequeno e médio porte. Dentre as que fornecem tais orientações, em países como França, Irlanda e Espanha, o auxílio também vem na forma de canais de comunicação, comumente através de FAQs, formulários prontos, *templates* de políticas de privacidade, *to-do lists* e canais telefônicos para o esclarecimento de dúvidas de pequenos empresários.

[10] JASMONTAITĖ-ZANIEWICZ, Lina et al. The GDPR made simple(r) for SMEs, p. 28. Disponível em: < https://library.oapen.org/bitstream/handle/20.500.12657/46614/Handboek_GDPR_ENG_HR-cert-febr4.pdf?sequence=1 >

[11] Data Protection: Better rules for small business. Disponível em: <https://ec.europa.eu/justice/smedataprotect/index_en.htm>.

[12] JASMONTAITĖ-ZANIEWICZ, Lina et al. The GDPR made simple(r) for SMEs, p. 24. Disponível em: < https://library.oapen.org/bitstream/handle/20.500.12657/46614/Handboek_GDPR_ENG_HR-cert-febr4.pdf?sequence=1 >

Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	De acordo com a LGPD, o registro é definido como obrigatório para todas as atividades de tratamento de dados, não sendo feitas exceções para qualquer categoria de agente ou atividade específica. Ocorre que a depender do porte da organização, manter um registro das operações de tratamento de dados representa custo bastante oneroso, já que a manutenção de elevados volumes de dados aumenta sensivelmente os custos de armazenagem de informações por parte das empresas de pequeno porte. Além disso, vale ressaltar que a LGPD não baliza um modelo claro e estruturado de registro que possa ser implementado pelos agentes econômicos com confortável grau de certeza, o que significa um terreno de riscos consideráveis, no qual as empresas podem vir a ser interpeladas futuramente, pela Autoridade, por omissões ou irregularidades em registros em razão de falta de maior orientação. Experiências internacionais já citadas mostram que em jurisdições como Colômbia e União Europeia a obrigação de um registro das operações de tratamento de dados pessoais foi dispensada para agentes de pequeno porte, salvo hipóteses bastante específicas como o tratamento massivo de dados e a utilização de dados sensíveis. Exceções similares para pequenos agentes econômicos no Brasil seriam bem-vindas – especialmente em face dos riscos, já citados, que a manutenção de registros conforme o art. 37 coloca para os agentes de tratamento. Outro exemplo positivo da experiência europeia está no entendimento exarado pelo Working Party 29 sobre o registro de atividades de tratamento por empresas de pequeno porte[13]. O órgão recomendou que, diante da criação de um novo encargo administrativo, seria recomendável que as Autoridades de Proteção de Dados adotassem uma postura cooperativa com relação ao registro, disponibilizando ferramentas e criando um modelo simplificado que poderia ser utilizado por pequenos negócios na manutenção dos registros de suas atividades.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Mais uma vez, o principal impacto relacionado à nomeação de um encarregado para agentes de pequeno porte é o custo. O fato de o contratado ter de ser uma pessoa independente é visto com preocupação, tendo em vista que isso pode levar à necessidade de duplicação de cargos e também considerando quão onerosa pode ser a mão-de-obra especializada para essa função. Há também muita incerteza quanto ao escopo exato da atividade do encarregado, bem como quanto ao tipo de vínculo que deverá guardar com a empresa - há nos debates desde posições propugnando pela necessidade de independência completa de qualquer instância decisória que

[13] ARTICLE 29 DATA PROTECTION WORKING PARTY. POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR. Disponível em: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045>.

	não a própria direção da empresa, até aquelas menos radicais que entendem que o encarregado poderia, inclusive, ser uma pessoa jurídica, contratada pontualmente para resolver questões específicas. A possibilidade de liberação da exigência de agentes de pequeno porte de designar o encarregado seriam possíveis medidas de flexibilização que ajudariam os pequenos negócios do setor de radiodifusão, uma vez que não implica custos adicionais. Vale lembrar que, conforme previsão do Artigo 41, § 3º, da LGPD, a ANPD pode estabelecer normas complementares sobre hipóteses de dispensa da necessidade de indicação de encarregado, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. Nesse sentido, a experiência europeia, já citada acima, pode ser interessante como referência, já que o GDPR estabeleceu exceções para empresas que não têm o tratamento de dados como parte de suas atividades essenciais, isto é, como atividades primárias das empresas, como é o caso das empresas membras da Abert.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	A elaboração de relatórios de impacto à proteção de dados pessoais decorre de análise de riscos a partir de diversos elementos associados ao tratamento de dados pessoais. Trata-se, portanto, de documento que depende de amplo conhecimento sobre legislação de proteção de dados pessoais. Para agentes de pequeno porte, portanto, sua elaboração implica em relevantes custos – seja para a formação de funcionários internos aptos a elaborar o documento, seja pela contratação de consultoria externa para o auxílio na sua elaboração. Entende-se que a regulamentação do tema pela ANPD, conforme prevista na Agenda Regulatória da Autoridade, terá o potencial de esclarecer o escopo e as circunstâncias em que a elaboração do documento é obrigatória, reduzindo as consideráveis dúvidas interpretativas que pairam sob o tema. É claro hoje na legislação que o relatório não se justifica para todo e qualquer tipo de tratamento de dados pessoais, portanto esse passo de definir com clareza as regras gerais e determinar quando ele será efetivamente solicitado pela autoridade já seria extremamente positivo para o setor empresarial – inclusive para empresas que não apenas as de pequeno porte. Para agentes de pequeno porte, por sua vez, o estabelecimento de regime diferenciado poderia se dar a partir de eventuais hipóteses de dispensa ou pela criação de modelo simplificado do

	relatório. Como dito, na medida em que fique claro quais as hipóteses nas quais o relatório é essencial, é possível que algumas pequenas empresas de pronto compreendam que boa parte dos tratamentos levados a cabo por elas não seriam de toda forma sujeitos a essa obrigação. Além disso, a ANPD poderia auxiliar estes agentes de pequeno porte a partir da criação de modelos e *templates* para relatórios, que reduziriam os custos associados à elaboração do documento. Isso também auxiliaria as empresas na medida em que deixaria muito mais explícito quais são as preocupações mais prementes da autoridade que definitivamente precisariam ser endereçadas quando da elaboração do relatório
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?	A Abert entende que a LGPD restringe o requisito de consentimento dos pais ao tratamento de dados pessoais de crianças, conforme literalidade do §1º art. 14 da lei – ou seja, essa regra certamente não se aplica a adolescentes. Ainda, entende-se que seria importante a atuação da ANPD no sentido de prever algumas flexibilizações a referido consentimento e também orientações para que a prova de identidade dos pais ou responsáveis legais não represente motivo para burocratização demasiada, o que é especialmente preocupante no caso dos agentes de pequeno porte. De toda forma, é inquestionável que há uma grande dificuldade operacional e de custo nesses casos, pois os sistemas devem apresentar maior rigor, seja na coleta, seja no acompanhamento do ciclo do tratamento dos dados pessoais e sensíveis.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Pensar em um programa de governança de dados significa pensar em apenas uma ponta de todo um conjunto de práticas variadas, que constitui a governança num sentido mais amplo. Elaborar políticas internas, delinear modelos de supervisão, estabelecer protocolos de reação a diferentes problemas, realizar análises de risco constantes, tudo isso compõem uma lógica de governança que simplesmente não faz parte do cotidiano da esmagadora maioria dos agentes econômicos de pequeno porte no Brasil. É evidente que agentes de pequeno porte buscarão adequar-se à legislação dentro de suas condições. Entretanto, é necessário agir com muita cautela ao exigir de pequenos negócios uma complexa implementação de políticas de governança de dados, sob pena de impor a eles gastos excessivos e desproporcionais que podem comprometer suas atividades.

	Ainda, a longo prazo, muitas dessas empresas de pequeno porte compreenderão que adotar programas do tipo será benéfico para seus negócios, tendo em vista que isso trará maior confiança dos consumidores e prevenirá possíveis incidentes de violação dos direitos de titulares de dados, que podem implicar multas para os agentes econômicos. Para se chegar nesse ponto, entendemos que a atuação da ANPD deve se dar, sobretudo, na forma de comunicação e orientações, muito em linha com experiências internacionais citadas, fornecendo guias práticos de implementação, modelos de procedimentos e instrumental de governança, bem como disponibilizando FAQs em seu site para esclarecer os benefícios e passo-a-passo para implementar um programa do tipo. Sabendo da realidade dos empreendimentos de pequeno porte brasileiros e considerando a delicada situação econômica atual, com a pandemia, é fundamental tornar a implementação de programas de governança de dados a mais cooperativa e flexível que se conseguir.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Também aqui, o custo para implementação da medida é o principal impacto que desperta receio entre os pequenos empresários do setor de radiodifusão. As emissoras de pequeno porte contam com faturamento modesto, sendo seu orçamento bastante contingenciado. Dessa forma, custear uma política de segurança de dados pode ser inviável para esses empresários. Para além disso, observa-se insegurança em relação a que constituiria exatamente uma política de segurança suficiente e quais seus parâmetros mínimos. Dado que ainda não existe uma definição mais ampla quanto a quais serão os requisitos que a ANPD implementará em matéria de segurança de dados pessoais, essa preocupação é compreensível. Tanto é que o assunto está sendo objeto de uma outra Tomada de Subsídios, iniciada nos últimos dias pela Autoridade[14]. Assim, a política de segurança de dados pessoais nas pequenas empresas deve ser pensada de modo a promover um encontro entre as disposições legais e a compreensão e percepção de riscos à segurança da informação por parte dos agentes econômicos. Deve-se encarar essa obrigação como uma porta de entrada, que permita a esses agentes relacionar adequadamente suas atividades de tratamento com as disposições legais, com níveis de proteção alinhados com os riscos representados pelas atividades exercidas pelos agentes.

[14] Tomada de Subsídios 2/2021, publicada no dia 22/02/2021, conforme Notícia no site da ANPD: https://bit.ly/3pUG7ue

Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	Tal como os programas de governança de dados, comentados em questão anterior, a avaliação sistemática de riscos também não faz parte do cotidiano da maior parte das micro e pequenas empresas do Brasil. Dar cabo de uma avaliação de risco não é simples e significa estabelecer um conjunto de procedimentos como mapear atividades de tratamento de dados, matrizes de riscos claras conforme tipo de atividade e estabelecer solidamente um plano de adequação à legislação de proteção de dados. Tudo isso, evidentemente, exige um conhecimento profundo da legislação, suas definições, abrangência e aplicação, conhecimento este que custa caro, seja capacitando e/ou contratando funcionários especializados, seja terceirizando a atividade para consultores técnicos e jurídicos. Mirando o exemplo das autoridades europeias, a ANPD poderia elaborar guias práticos, com linguagem simples, informando sobre a implementação de procedimentos que constituem uma avaliação sistemática de riscos, bem como oferecer modelos de documentos (inventário de dados, matrizes de riscos etc.) que possam ser aproveitados e preenchidos pelos agentes de pequeno porte. As exigências legais desse tipo de avaliação devem ser flexibilizadas ao máximo e, preferencialmente, classificar os agentes de pequeno porte pelo volume e/ou tipo de dados com que lidam, estabelecendo assim um conjunto de obrigações mais justo e condizente com a prática empresarial de cada um.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	A portabilidade de dados pessoais é um dos direitos dos titulares de dados pessoais que mais suscita dúvidas por agentes de tratamento de dados – incluindo questionamentos sobre o que este direito significa precisamente e como deve ser cumprido. Uma das especificidades do direito à portabilidade de dados pessoais é que este possui um relevante elemento técnico – a possibilidade de transmissão de dados pessoais entre fornecedores depende da utilização de padrão de dados pessoais comum. Neste sentido, a regulamentação do tema pela ANPD mostra-se central para a garantia de sua efetividade.

	Ainda, um dos questionamentos sobre este direito é se ele requer a transmissão direta das informações através de APIs ou caracteriza mero direito de acesso aos dados pessoais em formato interoperável. Para agentes de pequeno porte, obrigação de estabelecimento de mecanismos de transmissão direta de dados pessoais seria excessivamente custosa. Neste sentido, entende-se que é relevante que a regulamentação do tema dos direitos dos titulares de dados pessoais pela ANPD leve em consideração os custos associados à sua implementação, para que a medida não crie barreiras à entrada e custos de transação para novos agentes. Uma saída, por exemplo, seria o estabelecimento de direito à portabilidade simplificado no caso de agentes de pequeno porte – o direito de acesso aos dados pessoais em formato interoperável teria o potencial de atender ao relevante propósito regulatório da portabilidade, isto é, de redução de custos de troca. De maneira geral, entendemos que uma sistemática bem delineada precisa ser desenhada e assim confira-se aos agentes tempo apropriado para adaptação. O exemplo do open banking, sendo hoje implementado pelo Banco Central, demonstra a complexidade do tema. Mesmo instituições financeiras de grande porte, com sistemas altamente desenvolvidos, estão precisando de longo prazo e de diversas rodadas de discussão antes da efetiva implementação da portabilidade de dados. É muito provável que esse cenário se repita setorialmente.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	Acreditamos que a utilização de *sandboxes* regulatórios poderia ser uma alternativa interessante para a Autoridade fomentar a inovação entre empresas de pequeno porte. Os *sandboxes* permitem que, num determinado ambiente regulatório de testes, empresas com modelos de negócios inovadores ou em transformação, e nas fronteiras do arcabouço regulatório vigente, testem seus projetos e operem em caráter temporário, com supervisão constante das autoridades e maior liberdade de iniciativa. Num contexto de aceleradas transformações sociais e econômicas, é fundamental que os governos trabalhem para garantir que a revolução digital aconteça de uma forma que amplie ao máximo seus benefícios e minimize os riscos. Em matéria de proteção de dados, isso significa

	viabilizar a inovação baseada em dados e ao mesmo tempo garantir o uso responsável de informações pessoais pelos agentes do mercado[15]. A perspectiva de lançar um produto novo sabendo da existência de regimes regulatórios flexíveis, a oportunidade de construir um diálogo proveitoso com a ANPD e a construção de um ambiente que passa a mensagem de estar aberto para a inovação, são alguns dos muitos benefícios que a adoção de *sandboxes* regulatórios teria no arcabouço da proteção de dados no Brasil. Como já mencionado, a Autoridade de Proteção de Dados no Reino Unido (ICO) vem implementando em fase de testes um modelo de *sandbox* para matéria de proteção de dados e privacidade. Também é uma experiência que já está em andamento em outros setores regulados do Brasil, o que tornaria possível até mesmo um intercâmbio entre Autoridades. A Superintendência de Seguros Privados (Susep), a Comissão de Valores Mobiliários (CVM) e o Banco Central (Bacen) estão todos desenvolvendo suas regras e cronogramas específicos, sendo que as iniciativas do Bacen e da CVM devem começar ainda em 2021[16].
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. 1º. As microempresas, empresas de pequeno porte, startups autodeclaradas como de caráter incremental ou disruptivo e empresas de inovação autodeclaradas como de caráter incremental ou disruptivo estarão sujeitas a procedimentos simplificados e diferenciados, nos termos do artigo 55-J, XVIII da Lei nº 13.709/2018, conforme definidos nesta Resolução. Art. 2º. As microempresas, empresas de pequeno porte, startups autodeclaradas como de caráter incremental ou disruptivo e empresas de inovação autodeclaradas como de caráter incremental ou disruptivo estarão isentas de cumprimento das normas da Lei nº 13.709/2018 desde que: I – possuam menos de x [a serem discutidos na Consulta Pública] funcionários; e II – tenham faturamento inferior a x [a serem discutidos na Consulta Pública] reais.	

[15] CENTRE FOR INFORMATION POLICY LEADERSHIP HUNTON ANDREWS KURTH. Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice. Disponível em: < https://bit.ly/37JkIht>.

[16] NOOMIS CIAB FEBRABAN. Brasil inicia primeiros programas de Sandbox Regulatório. Disponível em: <https://noomis.febraban.org.br/temas/regulacao/brasil-inicia-primeiros-programas-de-sandbox-regulatorio>.

Parágrafo único. Também estão isentos do cumprimento todas as empresas elencadas no caput, cujo tratamento de dados pessoais não tenha finalidades comerciais, ou seja, destine-se exclusivamente a atividades administrativas ou para contato com usuários dos bens e serviços ofertados. Art. 3º. As microempresas, empresas de pequeno porte, startups autodeclaradas como de caráter incremental ou disruptivo e empresas de inovação autodeclaradas como de caráter incremental ou disruptivo não abarcadas pelas disposições do artigo 2º farão jus a procedimentos simplificados e diferenciados quando, cumulativamente: I – não realizarem tratamento de dados pessoais sensíveis, a menos que tal tratamento seja exclusivo para atividades administrativas da pessoa jurídica; II – não realizarem tratamento de dados pessoais de mais de x titulares de dados ao ano.
Art. Xxxx ....

Tomada de Subsídios 1/2021

Thomaz Côrte Real [redacted]

seg 01/03/2021 21:11

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

Cc: Rodolfo Fucher <rodolfo.fucher@abes.org.br>; Manoel Santos e <manoel.santos@abes.org.br>;

1 anexo

ABES_contribuicoes_PME_ANPD187918.pdf;

À
Autoridade Nacional de Proteção de Dados - ANPD
Exmo. Diretor Presidente Waldemar Gonçalves Ortunho Junior
Esplanada dos Ministérios, Bloco C, 2º andar
CEP 70297-400 - Brasília – DF.

Senhor Diretor Presidente Waldemar Gonçalves Ortunho Junior,

ABES - Associação Brasileira das Empresas de Software, vem pelo presente apresentar contribuições referente a tomada de subsídios nº 1/2021, que trata da tomada de subsídios sobre a regulamentação da aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

Colocando-nos à disposição para quaisquer esclarecimentos.

Atenciosamente,

[redacted] https://abessoftware.com.br/

[redacted]

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO
ABES – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

A **ABES - Associação Brasileira das Empresas de Software**, tem como propósito contribuir para a construção de um Brasil mais digital e menos desigual, no qual a tecnologia da informação desempenha um papel fundamental para a democratização do conhecimento e a criação de novas oportunidades para todos. Nesse sentido, com objetivo de assegurar um ambiente de negócios propício à inovação, ético, dinâmico e competitivo globalmente, sempre alinhado a sua missão de conectar, orientar, proteger e desenvolver o mercado brasileiro da tecnologia da informação, vem à presença de V.Exa., apresentar contribuições referente à tomada de subsídios nº 1/2021, que trata da tomada de subsídios sobre a regulamentação da aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos:

CONTRIBUIÇÕES

A. Faculdade na indicação do Encarregado pelo Tratamento de Dados Pessoais

O artigo 41 da LGPD prevê que o controlador deverá indicar encarregado pelo tratamento de dados pessoais. Na avaliação da ABES, a nomeação de um encarregado é incompatível com a realidade das microempresas e empresas de pequeno porte (“PMEs”), pois a contratação desse profissional envolve o desembolso de um salário de mercado e encargos trabalhistas, que em determinados casos, podem superar o faturamento de uma empresa desse porte.

Assim, a sugestão da ABES para esse item, seria a possibilidade das PMEs terem a faculdade de nomear um Encarregado, podendo ser o próprio sócio ou um profissional da estrutura da empresa, com acumulo de funções, sem que isso caracterize conflito de interesse, inclusive, podendo nomear um encarregado externo, empresa especializada que preste esse tipo de serviço.

B. Prazos diferenciados para atendimento da ANPD e solicitações de Titulares de Dados e comunicação de incidentes

Tendo em vista a enxuta estrutura e a reduzida capacidade financeira das PMEs, a flexibilização de prazos para atendimento da ANPD e solicitações de Titulares de Dados e comunicação de incidentes, devem ser flexibilizados.

A sugestão da ABES para esse item é que sejam estabelecidos prazos para cumprimento de obrigações pelas PMEs para atendimento da ANPD e solicitações de Titulares de Dados e comunicação de incidentes, que sejam, no mínimo, o dobro do conferido às demais empresas.

C. Mecanismos simplificados de Conformidade

De acordo com estudo feito pela CNI1, na União Europeia, as empresas com menos de 250 empregados não precisam manter registro das operações de tratamento de dados pessoais que realizam a menos que o processamento de informações seja a atividade regular da empresa, com real potencial de dano ao consumidor. Elas também são eximidas, em alguns casos, da obrigação de nomear um profissional específico para lidar com o tratamento dos dados2.

Várias autoridades de proteção de dados forneceram ferramentas práticas para facilitar a implementação da GDPR para PMEs com atividades de processamento de baixo risco. As autoridades de proteção de dados desenvolveram uma série de atividades para ajudar as PMEs a cumprir a GDPR, por exemplo, através do fornecimento de modelos para o processamento de contratos e registros para atividades de processamento, seminários e linhas diretas para consulta.3
Por certo, a manutenção do registro das operações de tratamento de agentes de pequeno porte exigirá uma infraestrutura tecnológica maior o que, por consequência, trará gastos adicionais à estas empresas.
A fim de facilitar o processo de adequação pelas PMEs e startups, considerando seus recursos limitado e ausência de pessoal especializado em proteção de dados no seu quadro de funcionários, a ABES sugere que seja regulamentado pela ANPD mecanismos simplificados de conformidade à LGPD às PMEs, como por exemplo a não obrigatoriedade de manter registro das operações de tratamento de dados pessoais que realizam, a menos que atividade econômica principal e regular da empresa, seja um modelo de negócios baseado no tratamento intenso de dados pessoais, com risco de dano em potencial e/ou constrangimento aos direitos e liberdades dos titulares de dados.

[1] https://noticias.portaldaindustria.com.br/noticias/economia/pequenas-empresas-tem-tratamento-especial-na-lgpd-na-europa-e-australia/

[2] https://www.cloudbric.com/blog/2018/01/gdpr-data-protection-officers/

[3] https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

Em um trabalho semelhante à EDPB (Comitê Europeu de Proteção de Dados), e considerando a baixa taxa de adesão à LGPD pelas pequenas e microempresas, a ANPD tem importante papel de orientar sobre os principais aspectos da Lei e os tópicos emergentes. É importante que seja criado um canal de contato, onde possam ser disponibilizadas *guidelines*, linhas de apoio e as ferramentas necessárias para que estas empresas possam se adequar à LGPD. A ABES coloca-se à disposição para colaborar com a ANPD, nas atividades de orientação e educativas para o mercado.

Por fim, a ABES ressalta que a LGPD foi um passo essencial para o país avançar rumo a uma efetiva aplicação do direito à proteção de dados pessoais na sociedade brasileira e que objetivo das contribuições ora apresentadas não é excluir a aplicação da lei às PMEs, mas sim, como a própria Nota Técnica nº 1/2021/CGN/ANPD menciona, garantir o direito de privacidade dos dados pessoais dos titulares que traga equilíbrio entre as regras constantes da LGPD e o porte do agente de tratamento de dados, buscando incentivar a inovação e o desenvolvimento econômico.

Colocando-nos à disposição para quaisquer esclarecimentos.

Atenciosamente,

Rodolfo Fücher
Presidente Executivo
ABES – Associação Brasileira das Empresas de Software
Por um Brasil mais digital e menos desigual

Tomada de Subsídios 1/2021

Thomas Kefas de Souza Dantas [redacted]

seg 01/03/2021 22:53

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

1 anexo

Modelo_envio_de_contribuicoes_PME_280121 - v.4.docx;

Caros.
O Grupo de Estudos em Direito Civil da Sociedade em Rede, da Faculdade de Direito da Universidade de São Paulo, coordenado pelo Professor Dr. Eduardo Tomasevicius Filho, vem, por meio deste, colaborar com a Tomada de Subsídios 1/2021;

Segue colaboração em anexo.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Grupo de Estudos em Direito Civil da Sociedade em Rede / Faculdade de Direito da Universidade de São Paulo

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	**Criar um ambiente regulatório que não prejudique o desenvolvimento de novas tecnologias e negócios e que ao mesmo tempo não estimule a violação da LGPD e assunção dos riscos relacionados, mas que, pelo contrário, sirva de estímulo para o respeito às normas de proteção de dados.** **Entrave inicial para o treinamento de experts em dados (áreas jurídica, de negócios e de tecnologia) em vista das obrigações legais, sendo ainda mais difícil para as iniciativas pequenas. De outro lado, isso significa o desenvolvimento de novos nichos de mercado ligados a estas áreas de dados, gerando outras iniciativas econômicas e consequentemente postos de trabalho;** **Enfrentar o problema dos dados já coletados pelas empresas, uma vez que foram coletados em um cenário anterior à LGPD podem ser considerados uma vantagem competitiva em relação às novas *startups*, implementar medidas de fiscalização nas empresas;**
Existem sugestões para endereçamento do problema?	**Sim, elaborar um regulamento que crie obrigações diferenciadas para *startup*s em relação ao tratamento de dados, considerando o porte e a realidade daquelas, além de criar medidas específicas de suporte e vigilância da ANPD às *startups*, o que vai ocasionar, na prática, o respeito às normas de proteção de dados.**

	Para endereçamento apropriado do problema é necessário complexificar a cadeia e estrutura regulatória, valendo-se de diferentes atores e instrumentos. Neste sentido, em diversos documentos a OCDE defende a distinção entre três camadas de intervenção sobre o mercado. Dentre eles destacamos o documento "Relationship between regulators and competition authority", que segmenta a regulação em três níveis distintos: a) regulação técnica (pela qual o órgão responsável está incumbido de criar ou dar continuidade a aplicação de normas destinadas a compatibilização de preocupações múltiplas envolvendo temas específicos do setor); b) regulação econômica (pela qual o órgão comprometido pode adotar políticas de preço, quantidade, qualidade, definições de acesso e níveis adequados de proteção aos interesses dos consumidores); e c) regulação concorrencial (quando poderá se auferir posturas mercadológicas relacionadas a condutas anticoncorrenciais e controle de estruturas). Uma solução proposta seria a criação de uma linha de fomento à atividade empresarial, nos moldes do projeto de inserção de "pesquisadores na empresa", onde o Estado poderia arcar com parcialmente com o custo de inserir um pesquisador da área de LGPD e Segurança da Informação nas M.E. e E.P.P, principalmente aquelas que tratem dados sensíveis, como forma de mitigar os custos operacionais de implementação para esse público específico.
Quais são as oportunidades relacionadas ao tema?	Dar um tratamento adequado, em conjunto e não conflitante dos temas de proteção de dados e *startups*, aproveitando as normas já existentes sobre o tema e as normas que possam vir a existir, sobretudo o Marco Legal das *Startups* que está em discussão no Congresso Nacional, aproveitando o diálogo entre as normas de maneira a propiciar maior segurança e *compliance* às normas de proteção de dados sem prejudicar o desenvolvimento de modelos de negócios inovadores. Incentivar que o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) possui um trabalho primordial no incentivo e acompanhamento dos pequenos negócios. A intenção é propor à entidade que, entre os serviços já oferecidos, elenque a formação de ao menos uma pessoa para a adequação do empreendimento à Lei Geral de Proteção de Dados, ressaltando a importância e necessidade de manter a empresa sempre de acordo com esta norma. Multiagencialidade: Proteção de Dados é um regime normativo que clama o envolvimento de outros ramos do direito: consumidor, concorrência, civil, criminal, razão pela qual possui ampla gama de efeitos. Tal fato reforça a necessidade de

	investigação do assunto a partir de uma perspectiva transversal dos fenômenos jurídicos e um respectivo entrelaçamento das autoridades brasileiras (CADE, ANPD, ANATEL, Senacon e outros) para o enfrentamento de situações que se complementam. Ainda mais, a formulação de regimes normativos apropriados também perpassa a inclusão de outros sujeitos, tais quais os próprios micro e pequenos empresários. Portanto, o tema suscita uma grande possibilidade de maior representatividade de interesses;
Quais são as experiências internacionais sobre o tema?	A GDPR exime as empresas ou instituições com menos de 250 empregados de manter registro do tratamento de dados, exceto se o tratamento realizado provavelmente resulte em risco aos direitos e garantias dos titulares, o tratamento não seja ocasional, o tratamento inclua o que chamamos de dados pessoais sensíveis e/ou dados criminais.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Inicialmente, devem ser utilizados como base os mesmos critérios de qualificação como *startup*, conforme aprovados no Marco Legal das Startups (Art. 4º). Após a qualificação como *startup*, esta deve buscar o enquadramento como agente de tratamento de dados de pequeno porte, devendo ser utilizado, nesse segundo momento, apenas um critério negativo e objetivo: a empresa que realize o tratamento de dados pessoais sensíveis não poderá ser qualificada como agente de tratamento de dados de pequeno porte.
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)?	Conforme pesquisa realizada, ainda não há atuação efetiva e concreta da União Europeia sobre o tema, estando o assunto limitado à previsão acima detalhada da GDPR de tratamento diferenciado às *SMEs*. As instituições e órgãos da União, bem como os Estados-Membros e respectivas autoridades de supervisão, são incentivados a ter em conta as necessidades específicas das micro, pequenas e médias empresas na aplicação da lei. Atenção especial para as necessidades específicas das micro, pequenas e médias empresas em relação: a criação de mecanismos de certificação de proteção de dados e de selos e marcas de proteção de dados, a elaboração de códigos de conduta, etc;
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	Os agentes econômicos de pequeno porte temem não suportar o impacto de alguém tão especializado em sua folha. O custo de bons profissionais tende a ser impeditivos para manutenção desses negócios no mercado. Tal fato pode afetar negativamente a evolução do número de M.E e E.P.P que surgem no mercado. A proteção de dados poderá funcionar como barreira à entrada de pequenos players no mercado.

Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	**Os custos de nomeação de um encarregado e de implementação da LGPD se mostram impeditivos quando relacionados à M.E. e E.P.P. Em pesquisa realizada com agentes econômicos diversos, nas EPPs, há um maior grau de desconhecimento da lei, dificuldade de encontrar um profissional para implementação por preços que estejam dentro do apertado orçamento dessas empresas.**
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	**Os custos de implementação da LGPD pode se tornar um problema, em especial para M.E. Em nossas pesquisas, além da dificuldade de encontrar profissionais capacitados no mercado, os preços praticados para elaboração de relatório de impacto e implementação da LGPD são os fatores que impedem a implementação da LGPD em M.E. e E.P.P.**
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?	
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	**Sugerimos a elaboração de um guia de processo simplificado de adequação para M.E. e E.P.P que tratem de dados sensíveis, que aponte soluções de segurança e de adequação à tais empresas, com suporte governamental em programas de implementação de pesquisadores na empresa como forma de fomento à adequação.**

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx Após qualificação como startup, M.E ou E.P.P na forma da lei, o agente deve buscar seu enquadramento como... agente de tratamento de pequeno porte, desde que não realize tratamento de dados sensíveis.
Art. Xxxx .A startup, M.E. ou E.P.P que realizar tratamento de ...dados sensíveis não terá benefícios dados aos agentes de tratamento de pequeno porte, contudo, terão prioridade em programas de suporte governamentais que visem auxiliar sua adequação à LGPD.

Tomada de Subsídios 1/2021

Fernanda Girardi Tavares [redacted]

seg 01/03/2021 22:59

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

1 anexo

Contribuicoes_FEDERASUL PME_280121 (2) (2).pdf;

Prezados,

em nome da **Federação das Entidades Empresariais do Rio Grande do Sul – FEDERASUL** e na condição de coordenadora da Comissão de Proteção de Dados da entidade, encaminho as contribuições da FEDERASUL com relação à regulamentação da aplicação da LGPD para microempresas, empresas de pequeno porte e iniciativas empresariais autodeclaradas startups no âmbito da Tomada de Subsídios 1/2021.

Estamos à disposição para as discussões subsequentes quanto ao tema.

Atenciosamente, Fernanda

SOUTO CORREA ADVOGADOS

Fernanda Girardi Tavares
[redacted]
www.soutocorrea.com

BRASIL | São Paulo | Rio de Janeiro | Porto Alegre | Brasília

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: FEDERASUL – Federação das Entidades Empresariais do Rio Grande do Sul

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	Os custos associados ao cumprimento das exigências da LGPD, além de um possível desincentivo às startups quanto ao desenvolvimento de novos negócios em campos envolvendo o tratamento de dados em virtude dos custos transacionais e riscos associados (tais como as penas pecuniárias e custos para o cumprimento das demais obrigações regulatórias).
Existem sugestões para endereçamento do problema?	Sim. Apresentamos, abaixo, sugestões de temas que são julgados pertinentes para que sejam tratados de maneira particular e diferenciada quando direcionados a agentes de pequeno porte: 1. Estipulação de prazos mais dilatados, podendo consistir no dobro daqueles concedidos para os demais agentes de tratamento de dados, para o atendimento dos pedidos dos titulares de dados (art. 18, par. 3º e 5º da LGPD) e para comunicação de incidentes de segurança (art. 48, par. 1º da LGPD). 2. Dispensa da obrigação de nomeação de um encarregado de tratamento de dados. 3. Dispensa da obrigação de manutenção do registro das operações de tratamento de dados pessoais.

	4. Dispensa da apresentação do Relatório de Impacto à Proteção de Dados Pessoais. 5. Dispensa da obrigação de portabilidade de dados (art. 18, V, da LGPD). 6. Sanções administrativas: criação de uma etapa prévia à imposição de sanções, de orientação aos agentes de pequeno porte quanto à infração cometida. 7. Sanções administrativas: redução do percentual da multa pecuniária passível de aplicação aos agentes de pequeno porte (art. 52, II, da LGPD) para 0,2% da receita do agente (em vez do faturamento).
Quais são as oportunidades relacionadas ao tema?	Incentivo a micro e pequenas empresas, além das startups para que possam empreender em um ambiente regulatório atento às particularidades dessas empresas, sem que estejam sujeitas a custos incrementais.
Quais são as experiências internacionais sobre o tema?	- A GDPR europeia dispensa o agente de tratamento de dados quanto ao registro das atividades de tratamento quando a empresa contar com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional e não abranja dados sensíveis, ou dados pessoais relativos a condenações penais e infrações. - Na Austrália, por exemplo, a lei de proteção de dados não é aplicável para empresas com faturamento de até USD3 milhões, a menos que a atividade econômica se enquadre naquelas reputadas como sujeitas (estudo conduzido pela CNI: https://noticias.portaldaindustria.com.br/noticias/economia/pequenas-empresas-tem-tratamento-especial-na-lgpd-na-europa-e-australia/)
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	A proposta é que o critério para que um agente de tratamento de dados seja considerado de pequeno porte esteja atrelado à receita bruta anual auferida pelas empresas, de acordo com os conceitos de microempresas e empresas de pequeno porte, conforme as disposições estabelecidas no artigo 3º da Lei Complementar nº 123/2006, variando conforme a receita bruta auferida anualmente. Já as *startups* e empresas de inovação, de acordo com o artigo 65-A da LC 123/2006, seguiria o critério de autodeclaração como startups ou empresas de inovação. Após o primeiro exercício, as startups poderiam seguir as mesmas faixas de receita das micro e pequenas empresas para serem mantidas na categoria de agentes de pequeno porte. Cabe aqui a menção ao art. 4º do projeto de lei

	(PLP 146.19) que visa implementar o Marco Legal das Startups e do Empreendedorismo Inovador. Em havendo conversão do projeto em lei, os critérios ali previstos poderão ser seguidos para nortear o enquadramento das startups. Além disso, estariam abrangidos por essa categoria as pessoas físicas que atuam com tratamento de dados para fins econômicos.
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)?	-
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	O impacto é relevante na estruturação operacional das micro e pequenas empresas, que precisariam destinar recursos significativos para o cumprimento dessa exigência. A sugestão é que seja editada norma regulamentadora com a redução do catálogo de dados a serem mantidos, buscando-se simplificar tais registros.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	A obrigatoriedade da nomeação de um encarregado de dados redunda em incremento do quadro profissional (na maioria das vezes bastante reduzido), geração de ineficiência de pessoal e aumento significativo da folha de pagamento (especialmente considerando-se as estimativas de níveis salariais já divulgados). Ainda que o encarregado seja terceirizado, os custos da contratação de tal serviço oneram os agentes de pequeno porte.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Agentes de pequeno porte, na maioria das vezes, não dispõe de recursos para investimento em assessorias para permitir a estruturação dos dados tratados e a reunião de elementos para a elaboração de um relatório de impacto à proteção de dados. Sugere-se que tal venha a ser exigido somente daqueles agentes que tenham, independentemente do porte, como **atividade econômica principal**, o tratamento de dados.
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?	Os agentes de tratamento de dados de pequeno porte não reúnem condições para cumprir com todas as obrigações regulatórias previstas, hoje, de maneira indistinta a todos os operadores e controladores.

Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Parece salutar que mesmo os agentes de pequeno porte estruturem programas de governança de dados, inclusive com o apoio de entidades representativas, para que possam promover tal gerenciamento de modo simplificado, mas norteado pela segurança da informação. Podem ser lançadas diretrizes e padrões de segurança mínimos pela ANPD para prover maior previsibilidade e minimizar os custos com consultorias nesse sentido. Além disso, o incentivo a campanhas educacionais para conscientização do corpo funcional mostra-se relevante, inclusive entre os agentes de pequeno porte.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Mostra-se adequado que mesmo os agentes de pequeno porte implantem políticas de segurança relativas à proteção de dados pessoais.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	A exigência da avaliação sistemática redunda também redunda em incremento de custos transacionais para os agentes de pequeno porte. Sugere-se que haja uma flexibilização de tal diretriz.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Custos de implantação de sistemas intercambiáveis e compatíveis para permitir a portabilidade.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	Um marco regulatório que assegurasse menores custos transacionais e que permitisse a empresas de pequeno porte atuarem de modo competitivo no mercado. A preocupação com a proteção de dados e privacidade deve ser uma constante, mas não um empecilho ao empreendedorismo.
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. 5º. XX - **Agente de tratamento de pequeno porte**: controlador ou operador que seja enquadrado como microempresa ou empresa de pequeno porte em conformidade com os critérios estabelecidos pela Lei Complementar 123/2006 ou norma que venha a sucedê-la; as iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e que possuam receita bruta em conformidade com os limites estabelecidos para microempresa ou empresa de pequeno porte; e a pessoa natural que promove o tratamento de dados para fins econômicos.
Art. 41. §4º. Ficam dispensadas da indicação de encarregados de dados os agentes de tratamento de dados de pequeno porte.

Tomada de Subsídios 1/2021

miele@ibcibr.com.br

seg 01/03/2021 23:26

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

Cc: contato@ibcibr.com.br <contato@ibcibr.com.br>;

1 anexo

20210301_IBCI_Consulta Pública - ANPD_revfin_encrypted_.pdf;

Prezados, boa noite!

Com o intuito de contribuir para com a tomada de subsídios sobre a regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte, o Instituto Brasileiro de Concorrência e Inovação encaminha pontuais comentários e contribuições.

Desde já renovamos os votos de estima e apreço, parabenizando todos pelo trabalho realizado.

Cordialmente,

Aluísio de Freitas Miele
Diretor - IBCI

São Paulo, 01 de março de 2021.

Aos
Excelentíssimo Sr. Dr. Diretor-Presidente, Waldemar Gonçalves Ortunho Junior,
Excelentíssima Sra. Drª. Coordenadora Geral de Normatização, Dra. Isabela Maiolino e
Excelentíssimo Sr. Dr. Rodrigo Santana dos Santos, Coordenador de Normatização

Autoridade Nacional de Proteção de Dados (ANPD) - Casa Civil da Presidência da República

Ref.: Contribuições Referente à Tomada De Subsídios nº 1 /2021

Exmo. Senhores,

O Instituto Brasileiro de Concorrência e Inovação - IBCI - é um *think tank* aberto e sem fins lucrativos criado em 2012 a partir da iniciativa conjunta de um grupo de Professores da Pontifícia Universidade Católica de São Paulo (PUC-SP) e da Universidade de São Paulo (USP). O IBCI prega valores de livre iniciativa, livre concorrência, inovação, *level playing field* para a construção de uma sociedade mais justa, com mais bem-estar e menos desigualdade por meio de mercados abertos e competitivos.

Fazendo jus aos seus pilares de existência, o IBCI é composto por um quadro multidisciplinar e 100% paritário de diretores e diretoras, isto é, 50% mulheres e 50% homens, todos com reconhecido destaque em suas respectivas áreas de pesquisa, docência e atuação profissional.

O IBCI, nesta oportunidade, vem mui respeitosamente à presença de V. Exas. apresentar pontuais comentários e contribuições à tomada de subsídios sobre a regulamentação da aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, para microempresas e empresas de pequeno porte.

Nestes termos, reforça-se o entusiasmo com a seriedade e qualidade dos trabalhos realizados, conjugados à relevância do aprimoramento do sistema regulatório pátrio, em favor da proteção de dados, tratamento de dados, concorrência, competividade e das questões sensíveis referentes às micro e pequenas empresas de caráter disruptivo, solicitando seja recebida e apreciada a presente contribuição.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

Instituto Brasileiro de Concorrência e Inovação - IBCI

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	Perfil de Mercado Para um Adequado Controle de Dados

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	A presente tomada de subsídios apresenta em sua raiz a busca por um perfil de mercado dos agentes de pequeno porte (também denominados de pequenas iniciativas) com o objetivo de formular um adequado e proporcional controle de dados. Este objetivo encontra reflexos nos seguintes problemas ou desafios, os quais demandam soluções proporcionais e adequadas: ● Natureza das problemáticas: Existem três dificuldades, de natureza mais econômica, proporcionalmente maiores às pequenas iniciativas: i) custos para financiamento, ii) custos administrativos para cumprimento das diversas obrigações legais e iii) custos informacionais para obtenção de novas tecnologias (MENDES, 2016), somam-se ainda o custo constante de aprendizagem e acesso à informação, ambos relacionados à necessidade de capacitação e treinamento de colaboradores/funcionários; ● Potencialidade de ilícitos e danos: Pequenas iniciativas geram a priori menos danos à proteção de dados, devido a acesso restrito de dados, a um mercado com extensão geográfica reduzida e a menores transferências internacionais de dados, devendo ter obrigações proporcionais a sua realidade;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	● Falhas Informacionais: Existe uma série de informações técnicas e de mercado que os pequenos negócios não obtêm e que consequentemente geram um desfavorecimento em termos de estratégia de mercado quando competem com os grandes negócios, como custos, operadores, análises (riscos, potencialidade de ilícitos), entre outros fatores concorrenciais; ● Barreiras à Entrada: As barreiras de entrada são obstáculos de diversas naturezas e causas para negócios existentes ou novos negócios, podendo dificultar ou impossibilitar sua atividade em um dado mercado caso não enfraquecidas ou eliminadas. Sob esta abordagem, percebem-se estas barreiras de entrada como desafio e problema regulatórios relacionados ao tema: **(i)** Entrave inicial para o treinamento de experts em dados (áreas jurídica, de negócios e de tecnologia) em vista das obrigações legais, sendo ainda mais difícil para as iniciativas pequenas. De outro lado, isso significa o desenvolvimento de novos nichos de mercado ligados a estas áreas de dados, gerando outras iniciativas econômicas e consequentemente postos de trabalho; **(ii)** A LGPD pode se tornar mais uma das legislações que declaradamente tutelam as pequenas iniciativas em face das grandes iniciativas, mas que na realidade servem como reserva de mercado para estas;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

Existem sugestões para endereçamento do problema?	<u>Estruturas Regulatórias e Instituições</u> Para endereçamento apropriado do problema é necessário complexificar a cadeia e estrutura regulatória, valendo-se de diferentes atores e instrumentos. Neste sentido, em diversos documentos a OCDE defende a distinção entre três camadas de intervenção sobre o mercado. Dentre eles destacamos o documento *"Relationship between regulators and competition authority"*, que segmenta a regulação em três níveis distintos: a) **regulação técnica** (pela qual o órgão responsável está incumbido de criar ou dar continuidade a aplicação de normas destinadas a compatibilização de preocupações múltiplas envolvendo temas específicos do setor); b) **regulação econômica** (pela qual o órgão comprometido pode adotar políticas de preço, quantidade, qualidade, definições de acesso e níveis adequados de proteção aos interesses dos consumidores); e c) **regulação concorrencial** (quando poderá se auferir posturas mercadológicas relacionadas a condutas anticoncorrenciais e controle de estruturas). Para além destas três camadas, propomos ainda o estudo de viabilidade de inclusão de agentes privados, dotados estes de informações, conhecimentos e instrumentos próprios, capazes de reduzir os custos operacionais, bem como de atingir determinados resultados de maneira mais eficaz. Por tanto, algumas possíveis conclusões seriam:

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	• Regulação Técnica: No que diz respeito à cooperação técnica entre os órgãos que disciplinam a atividade econômica, é preciso pleitear um modelo que considere a capacidade de decisão das funções descritas (regulação técnica, econômica e concorrencial) com estruturas suficientemente aptas a garantir a eficiência das deliberações pretendidas para o setor privado, a fim de minimizar os efeitos comumente observados dentro da burocracia brasileira, tais como morosidade dos processos administrativos (responsáveis por gerar insegurança jurídica nos mercados), o "custo burocrático de transação" (presente nas operações realizadas entre instituições públicas) e o risco de conflito de competências resultante da atuação conjunta de diversos órgãos sobre o mesmo problema. Dentre os principais órgãos a serem considerados para eventual cooperação cita-se Conselho Administrativo de Defesa Econômica (CADE), Agência Nacional de Telecomunicações (ANATEL), Secretaria Nacional do Consumidor (SENACON); • Regulação Econômica: No que tange a adoção de medidas atreladas ao ambiente de mercado, dentre as quais a definição do próprio critério de não aplicação da LGPD aos agentes de pequenos portes, há de se ressaltar que pela ausência de informações adequadas os agentes públicos estão constantemente sujeitos a atribuírem decisões estritamente desconexas com a realidade ou exigência do mercado, razão pela qual uma análise do impacto regulatório é fundamental;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	• Regulação Concorrencial: Já em atenção aos impactos à concorrência, a cooperação institucional entre ANPD e outras agências de Estado, como o CADE, pode ser importante para delimitação apropriada quanto aos efeitos em empresas inovadoras e à garantia de competitividade no digital, marcado por tendências monopolizantes advindos da economia de escala, de escopo, bem como dos efeitos de rede – todos presentes nos grandes ecossistemas digitais; • Co-Regulação Público-Privada: Para além das entidades públicas, a União Europeia (Competition policy for the digital era, 2019) propõe a cooperação entre agentes públicos e privados, ante a assunção, pelos agentes de mercado - especialmente as plataformas privadas - de funções eminentemente regulatórias, como no caso de aspectos concorrenciais, política de pagamento e de anúncio no mercado interno às plataformas. Em face disto, comumente tem se atribuído modelos diferenciados de autorregulação regulada, como se depreende não só de normativas em vigor - como na 10ª emenda à lei contra restrições à concorrência alemã -, mas também de normativas atualmente em análise pela Comissão Europeia, como o *Digital Services Act* e o *Digital Markets Act*. O que chama maior atenção nestas normativas é a imposição de quesitos mínimos às cláusulas contratuais de plataformas privadas, a garantia de interoperabilidade e portabilidade, bem como imposição de padrões mínimos de contraditório e ampla defesa em reclamações internas. Ainda, há de se ressaltar que a lei

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	chinesa anti-monopólio instituiu o abuso do poder regulatório à autoridade concorrencial, buscando evitar regimes normativos prejudiciais por sistemas de *accountability.* A partir da inclusão de entidades privadas na regulação da proteção de dados, tanto ampliamos os instrumentos, quanto a capacidade de obtenção de informações a custo reduzido. Algumas possibilidades são: **(i)** regulamentação do art. 9º, §1º da MCI, que aborda eventuais hipóteses de tratamento diferenciado de pacotes de dados; **(ii)** mecanismos de incentivos disruptivos ao mercado, tal qual instituição de mandados de *Qui Tam*, em que agentes privados podem ser beneficiados com parcela da recuperação de ativos ou parcela da multa imposta pelo Governo quando da hipótese de participação na fiscalização e denúncia de violações à LGPD e normas a ela relacionadas; **(iii)** Cooperação regulatória entre plataformas e ANPD para garantia de tratamento favorecido a micro e pequenas empresas quanto taxas internas à companhia, requisitos mínimos obrigatórios de cumprimento normativo; *Sandbox* regulatório e institutos do MLSEI e da Nova Lei de Licitação

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	Na economia atual, as *startups* constituem agentes econômicos fundamentais para o desenvolvimento de novos bens e serviços com foco em inovação. Não raramente, suas dinâmicas criativas em diversas camadas de produção e aplicação de ferramentas dependem do uso e tratamento de dados. Esses agentes precisam lidar frequentemente com dilemas relacionados a diversas incertezas regulatórias ocasionadas pelo desenvolvimento dos seus modelos de negócios, que estão especialmente ligados ao incremento de soluções inovadoras em diversos mercados[1]. • Marco legal das Startups e do Empreendedorismo Inovador (MLSEI - PLP nº 249/2020): já estabelece diretrizes que consideram especialmente: (i) diretrizes para atuação do setor de inovação junto à administração pública; ii) medidas que favorecem a oferta de capital para investimento em empreendedorismo inovador e promovem um ambiente saudável para o desenvolvimento de *startups*; iii) criação de regras especiais para contratações e processos licitatórios que tenham como objetivo ofertar soluções inovadoras para a administração pública.

[1] Neste sentido, Cf. ALVES, S.G; PEREIRA. J. R. L. Marco Legal das Startups, LGPD e sandboxes regulatórios em colaboração: Os caminhos regulatórios interdisciplinares capazes de promover a inovação de novas empresas. In: portal de notícias **JOTA**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/marco-legal-das-startups-lgpd-e-sandboxes-regulatorios-em-colaboracao-21122020. Acesso em: 16 fev. 2021.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	Ocorre que além disso, o MLSEI traz também o mecanismo conhecido como **"Sandbox regulatório"**, que consiste em espaços de suspensão regulatória, onde o regulador oferece condições diferenciadas a determinadas pessoas jurídicas que recebem autorização temporária para desenvolver e testar modelos de negócios experimentais ou com tecnologia inovadora. O desenvolvimento dessas atividades deve ocorrer segundo o cumprimento de limites e critérios desenhados pela autoridade setorial que também irá monitorar e fiscalizar a evolução dessas dinâmicas no mercado em questão (art. 2º, II, MLSEI). • Cooperação entre órgãos para programas de *Sandbox* Regulatório: MLSEI prevê ainda a possibilidade de elaboração de acordos de colaboração entre agentes reguladores setoriais para que desenvolvam programas de *sandbox* transversais, ou seja, que possam permear mais de um âmbito regulatório, instituindo programas que alcançam competências distintas. O funcionamento do programa deverá estabelecer: (i) os critérios para seleção ou para qualificação do regulado; (ii) a duração e o alcance da suspensão da incidência das normas; e (iii) as normas abrangidas (art. 11 e incisos da MLSEI). • Nova Lei de Licitação e *startups*: destacamos, por fim, as possibilidades trazidas também pelo texto da Nova Lei de Licitações (PL 4.253/2020), recém aprovado pelo Senado e que aguarda sanção presidencial. Há tempos são discutidas entre especialistas as vantagens do uso do poder de compra

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	do Estado como instrumento de política de inovação, do ponto de vista da demanda. Nesse sentido, a nova lei considera que "*a demanda pública por bens e serviços privados não precisa ser apenas guiada pela busca do menor preço e dos impactos imediatos de curto prazo, mas ao contrário, deve se orientar pela busca do maior retorno para o Estado e para a sociedade. Daí, o uso estratégico das licitações e contratos como estímulo à inovação*". (Rauen, 2021). Por essa razão, o novo PL incorpora o chamado procedimento de manifestação de interesse (PMI) nas licitações e contratações administrativas em geral com o objetivo de fomentar soluções inovadoras. Art. 80. A Administração poderá solicitar à iniciativa privada, mediante procedimento aberto de manifestação de interesse a ser iniciado com a publicação de edital de chamamento público, a propositura e a realização de estudos, investigações, levantamentos e projetos de soluções inovadoras que contribuam com questões de relevância pública, na forma de regulamento (Artigo 80 da Nova Lei de Licitações) Isto significa que, diante da rápida evolução tecnológica que afeta as concessões e PPPs, é oferecida uma alternativa à Administração Pública para, na ausência de recursos para realização dos referidos

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	estudos, se manter ainda assim atualizada em relação às mais avançadas tecnologias e considerar as modalidades de negociação que envolvem as matérias de inovação (Rauen, 2021). Pontuamos, particularmente, o §4º do referido artigo que, nas palavras do Diretor de Estudos e Políticas Setoriais de Inovação e Infraestrutura do Instituto de Pesquisa Econômica Aplicada (Ipea), André Rauen, "*permite restringir o PMI a startups e ao fazê-lo apresenta a primeira definição, desde que sancionada pela Presidência da República, deste tipo de empresas na lei brasileira*": § 4º O procedimento previsto no caput deste artigo poderá ser restrito a startups, assim considerados os microempreendedores individuais, as microempresas e as empresas de pequeno porte, de natureza emergente e com grande potencial, que se dediquem à pesquisa, ao desenvolvimento e à implementação de novos produtos ou serviços baseados em soluções tecnológicas inovadoras que possam causar alto impacto, exigida, na seleção definitiva da inovação, validação prévia fundamentada em métricas objetivas, de modo a demonstrar o atendimento das necessidades da administração. ● É preciso estudar as vantagens e desvantagens de tal definição e verificar se a métrica da LGPD se aplicaria diante do cenário descrito pelo art. 80, caput e §4º, da Nova Lei de Licitação.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	Endereçamentos e Institutos da LGPD ● Previsão legal para LGPD criar regulação diferenciada: o artigo 55-J, inciso XVIII, da LGPD, fornece um instrumento legal para a criação de um *sandbox* regulatório destinado a regulação de dados, especialmente dirigido ao desenvolvimento de normas e procedimentos simplificados para ME, EPP e empresas com atividades experimentais e disruptivas no âmbito tecnológico, autodeclaradas *startups*. Seria possível então a ANPD articular uma política de ambiente regulatório experimental em cooperação com outras agências, como por exemplo ANATEL e BACEN; ● Padrões de Termos de Uso e Práticas Anticompetitivas: Recentes estudos na seara de regulação e concorrência têm demonstrado a abertura à práticas anticompetitivas a partir da formulação de termos de uso e políticas de privacidade (neste sentido: CONDORELLI, PADILLA, 2020). A temática suscita a relevância da garantia de governança de dados, quanto mais em face da utilização de pequenas empresas por parte de grandes agentes de mercado como expansão de seus interesses por intermédio de vias informais, viabilizando a coleta, processamento, importação e exportação de dados desregulada. Portanto, cumpre pensar critérios de quarentena para aplicação às empresas participantes de *sandbox* regulatório, ante a possibilidade de apropriação e captura destas vantagens por empresas dominantes;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	• <u>Conflitos de Interesses:</u> Há de se ressaltar neste ponto que a regulamentação do Encarregado de Dados Pessoais (DPO) configura ponto fulcral para evitar conflitos de interesses dentro da companhia, a viabilizar não só o devido cumprimento, mas uma estrutura corporativa que favoreça a denunciação quando das hipóteses de violação normativa. Por este motivo, é possível pensar em uma categoria diferenciada, com novos balanceamentos de direitos e deveres de DPO para hipóteses de aplicabilidade da LGPD a agentes de pequeno porte.
Quais são as oportunidades relacionadas ao tema?	<u>Perspectivas e Potencialidades</u> A regulamentação específica quanto a aplicabilidade de regimes normativos de proteção de dados em face de agentes de mercado de pequeno porte é ainda deveras incipiente em todo o globo. Por um lado, isto cria um vazio de experiências passíveis de comparação e respectivo aprimoramento em âmbito pátrio, mas por outro é possível afirmar que a abertura do tema também pode ser uma oportunidade de aprimoramento e harmonização do regime normativo, alçando a experiência brasileira como modelo internacional. Desta feita, propomos as seguintes considerações:

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	● Multinormatividade: Proteção de Dados é um regime normativo que clama o envolvimento de outros ramos do direito, como por exemplo: consumidor, concorrência, civil, criminal, razão pela qual possui ampla gama de efeitos. Tal fato reforça a necessidade de investigação do assunto a partir de uma perspectiva transversal dos fenômenos jurídicos e um respectivo entrelaçamento das autoridades brasileiras (*e.g.*, CADE, ANPD, ANATEL, Senacon) para o enfrentamento de situações que se complementam. Ainda mais, a formulação de regimes normativos apropriados também perpassa a inclusão de outros sujeitos, tais quais os próprios micro e pequenos empresários. Portanto, o tema suscita uma grande possibilidade de maior representatividade de interesses; ● Desenvolvimento Econômico: A regulação apropriada quanto a aplicabilidade do regime normativo de proteção de dados a micro e pequenos empresários é capaz de favorecer o crescimento econômico, reduzir custos de participação e entrada no mercado, bem como ampliar os agentes de tratamento de dados, respectivamente gerando competitividade, maior amplitude de interoperabilidade e portabilidade, sem prejudicar o desenvolvimento tecnológico; ● Pioneirismo: Ainda que o tema seja incipiente no mundo, a formulação de respostas normativas vai de encontro a necessidades e problemáticas enfrentadas internacionalmente, razão pela qual será oportunidade tanto para testar a formalização de instrumentos regulatórios inovadores, tornar-se

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	modelo exemplo ao mundo, bem como invocar a atenção e debate com diferentes agentes privados e público; ● Inovação: O Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) possui um trabalho primordial no incentivo e acompanhamento dos pequenos negócios. A intenção é propor à entidade que, entre os serviços já oferecidos, elenque a formação de ao menos uma pessoa para a adequação do empreendimento à Lei Geral de Proteção de Dados, ressaltando a importância e necessidade de manter a empresa sempre de acordo com esta norma.
Quais são as experiências internacionais sobre o tema?	*Benchmarking* À título de *benchmarking*, isto é, de busca das melhores ou possíveis prescrições de direito e suas aplicações relativas aos temas em pesquisa, apresentam-se as seguintes: ● Europa: GDPR estabelece em diversos pontos que as micro, pequenas e médias empresas devem ser tratadas de forma específica e com atenção especial, porém, em poucos pontos determina qual é o protocolo que deve ser seguido.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	• Austrália: Na Austrália, a Lei de Privacidade não se aplica à maioria das pequenas empresas, com faturamento anual de até US$ 3 milhões. Ela incide apenas em negócios específicos como operadores de bancos de dados de locação residencial. De todo modo, especialistas reforçam que apesar de em uma pequena empresa os problemas de proteção de dados não surgirem o tempo todo, é aconselhável que nomeiem um responsável pela proteção de dados, pois assim conseguem manter-se em conformidade e evitar problemas com o BDSG. Empresas precisam de um oficial de proteção de dados apenas se lidarem constantemente com o processamento automatizado de dados pessoais de pelo menos 20 pessoas. • África do Sul: Na África do Sul, percebem-se cautelas em face da proteção de dados pessoais mesmo estando a privacidade arrolada no capítulo do Bill of Rights da Constituição. O Protection of Personal Information Act (POPIA) de 2013 parcial e gradativamente entrou em vigor ao longo dos anos, sendo que apenas será totalmente aplicável em junho de 2021. A proibição de processamento dos dados pessoais não se aplica em alguns casos, como no propósito nacional da proteção de pessoas desfavorecidas por discriminação. Apesar da ressalva quanto a efeitos e de outras quanto a matérias, o POPIA não tratou especificamente sobre pequenos e médios negócios, tal como o fez a legislação de concorrência deste país em 1998 a título de comparação.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Critérios Para Definição de Aplicabilidade da LGPD a Agentes de Pequeno Porte Decerto que a definição de qualquer dos critérios possíveis para aplicabilidade da Lei Geral de Proteção de Dados agentes de pequeno porte implicará tanto em efeitos pretendidos, quanto em adversos. Não obstante, em que pese a incerteza acerca do tema, parece possível afirmar, a partir das experiências em outros ramos do direito, que a atribuição de critérios dinâmicos é fundamental agregando mais de uma seara de classificação, razão pela qual apontamos as possíveis possibilidades: ● Faturamento: Possibilidade de aplicação da LGPD à micro e pequenas empresas a partir de valor objetivo aferido da Lei Complementar 123/2006, ou de faturamento adquirido diretamente com a exploração de dados; ● Objeto social: Aplicação da LGPD a partir da relação do objeto social da empresa com tratamento de dados, ante a maior potencialidade de cometimento de violações nesta hipótese. ● Empregabilidade: Trata-se do critério adotado pela GDPR, especificamente em que foram excluídas da hipótese de aplicação do regime normativo de proteção de dados aquelas com menos de 200

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	empregados; Não obstante tratar-se de hipótese geral, cada país poderia fixar, em acordo à realidade nacional, critério diferenciado. Foi assim que França atribuiu hipótese mais severa, excluindo apenas empresas com menos de 20 empregados. Critérios Sob Uma Ótica Mais Ampliada ● Parâmetros diferenciados quanto a exigências internacionais em vista de possíveis incentivos; ● Grupos econômicos e de contratos associativos dos quais sejam parte os agentes de pequeno porte; ● Relevância na proteção de dados almejada considerando o controle e o tratamento efetivamente praticados; Flexibilização Dos Critérios ● Flexibilização dos critérios para patamares superiores (por exemplo, o dobro) no caso de atividade de marketing exercida exclusivamente para promoção do próprio negócio, na medida em que a perda deste marketing direto pode prejudicar severamente as receitas destes agentes (BOTHA; ELOFF; SWART, 2015).

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	<u>Exceção À Isenção Legal Dos Agentes De Pequeno Porte</u> ● Exceção para impor obrigação de dados com margem de discricionariedade (por faturamento, por objeto social, por ramo de mercado específico, ou por um conceito indeterminado) aos agentes de pequeno porte caso seja necessária à proteção de dados mediante motivação da Autoridade Nacional de Proteção de Dados;
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)?	<u>Modelo da União Europeia</u> Para nortear os próximos passos da Autoridade com base na forma em que a União Europeia encara o referido assunto, pontuou-se neste tópico dados relevantes da análise sob à ótica da GDPR, quais sejam: ● <u>Isenção da obrigação de manter registro:</u> Empresas ou instituições com menos de 250 funcionários estão isentas de manter um registro se (i) o processamento não for susceptível de representar um risco para os direitos e liberdades do titular dos dados; (ii) nenhuma categoria especial de dados for processada; ou (iii) o processamento é feito apenas ocasionalmente, conforme indicado no art. 30 (5) GDPR. Na prática, esta isenção raramente é aplicável;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	• <u>Emissão de notificações de violação em 72h</u>: há um incentivo aos controladores de dados para que estes realizem a emissão das notificações de violação dentro das 72 horas (a contar da descoberta), sob pena de multa de até 2% da receita global; • <u>Esclarecimento dos processamentos realizados</u>: incentivo à adoção de avisos de processamento justos, descrevendo a finalidade, a fundamentação, os destinatários, o tempo de armazenamento etc.; • <u>Atenção às necessidades peculiares dos menores no mercado</u>: as instituições e órgãos da União, bem como os Estados-Membros e respectivas autoridades de supervisão, são incentivados a ter em conta as necessidades específicas das micro, pequenas e médias empresas na aplicação da lei. Atenção especial para as necessidades específicas das micro, pequenas e médias empresas em relação: a criação de mecanismos de certificação de proteção de dados e de selos e marcas de proteção de dados, a elaboração de códigos de conduta etc.;
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	<u>Estímulos e Desestímulos Econômicos</u>

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	Se por um lado a implementação de programas de governança de dados é capaz de mitigar riscos de violação ao regime normativo de proteção de dados, por outro certamente a imposição de custos para entrada no mercado configura barreira à competitividade, em face do aumento de custos necessários para tanto. A consequência inevitável é a exigência de uma proporcionalidade entre ambos os objetivos, razão pela qual é possível concluir que: ● Redução de Riscos de Violação: A imposição de governança de dados aos agentes de pequeno porte é capaz de reduzir os riscos de violação ao regime normativo de proteção de dados. Trata-se de riscos certamente menos danosos que agentes de mercado de maior porte, bem como dotados de menor potencialidade de efeitos negativos a outras esferas para além da proteção de dados, como concorrência, aspectos civis e penais; ● Aumento de Barreiras à Entrada: Na medida em que a imposição de padrões mínimos de governança aumenta os custos de cumprimento normativo, decerto que a regulação do tema aumentará as barreiras à entrada no mercado, reduzindo a participação de agentes de mercado e, possivelmente, a competitividade do mercado;

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	● <u>Proporcionalidade entre Governança e Riscos:</u> A ponderação entre padrões de governança e riscos envolvidos é capaz de tanto prejudicar a concorrência, quanto aumentar o padrão competitivo entre as empresas, a depender do balanceamento de custos e benefícios envolvidos. Sugere-se, neste ponto,
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	<u>Instrumentos regulatórios</u> Por intermédio da complexificação da cadeia regulatória proposta no item "Existem sugestões para endereçamento do problema?" podemos repensar a natureza de instrumentos apropriados para promoção da inovação nos agentes de pequenos portes. Neste sentido, tanto a inclusão de agentes privados, quanto a utilização de novas tecnologias despontam como potenciais soluções para aprimoramento dos efeitos pretendidos. Em vista destas potencialidades, apontamos as seguintes possibilidades: ● <u>Guidelines:</u> A formulação de Guidelines é uma importante via de esclarecimento dos entendimentos das autoridades públicas, bem como de apontamento para condutas apropriadas pelos agentes privados. Neste sentido, sabidamente como mecanismos de *soft law*, são capazes de induzir o comportamento dos agentes. Portanto, a formulação de uma *guideline* específica aos agentes de pequeno porte seria importante mecanismo para redução das incertezas dos agentes de mercado, além

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

	do incentivo ao cumprimento normativo pela redução dos custos associados à obtenção de determinadas informações; ● Penalidades: Em se tratando a pena um dos instrumentos clássicos e essenciais do direito, é possível repensar hipóteses de sua aplicabilidade não só a partir de montante financeiro vinculado ao faturamento ou dano, mas também hipóteses de remédios comportamentais ou estruturais para saneamento de problemas em empresas de pequeno porte, evitando prejuízos financeiros que venham a prejudicar o andamento da atividade econômica; ● Cooperação técnica e institucional: A consideração das consequências regulatórias no âmbito concorrencial auxilia na árdua tarefa de encontrar uma equilibrada divisão de competências, o que diminui o conflito normativo entre entes e corrobora para o aproveitamento da experiência e capacidade técnica, promovendo a chamada "vigilância recíproca" entre as autoridades e a prevenção do "abuso de poder regulatório". Dentre os mecanismos de cooperação está a celebração de memorandos de entendimento, com análise conjunta dos potenciais efeitos dos atos normativos ou sancionatórios. Pontua-se ainda o papel da advocacia da concorrência, a qual influencia diretamente na elaboração de políticas setoriais desenvolvidas por Agências Reguladoras.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. 1º - A Autoridade Nacional de Proteção de Dados, quando da hipótese exclusiva de denúncia não anônima fundamentada por agente privado que resulte na recuperação de ativos pela Federação ou imposição de multa por descumprimento normativo, em qualquer de seus níveis, poderá destinar até 10% do montante total recuperado, ou da multa imposta, ao denunciante como mecanismo de incentivo à fiscalização e denúncia pelos agentes privados. §1º - Os critérios de destinação dos recursos recuperados ou das multas impostas aos denunciantes, bem como o regime de proteção ao denunciante e os procedimentos para aplicabilidade do instituto, serão especificados por intermédio de portaria específica. §2º - Na hipótese de denúncia manifestamente inepta e de efeitos negativos notórios ao denunciado, assim como na hipótese de denúncia reiterada não fundamentada ou não arrazoada, a Autoridade Nacional de Proteção de Dados poderá fixar multa pela prática abusiva de denunciação.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, S.G; PEREIRA. J. R. L. **Marco Legal das Startups, LGPD e sandboxes regulatórios em colaboração: Os caminhos regulatórios interdisciplinares capazes de promover a inovação de novas empresas.** In: portal de notícias JOTA. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/marco-legal-das-startups-lgpd-e-sandboxes-regulatorios-em-colaboracao-21122020. Acesso em: 16 fev. 2021.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

BOTHA, J. G.; ELOFF, Mariki M.; SWART, I. The effects of the PoPI Act on small and medium enterprises in South Africa. In: **2015 Information Security for South Africa (ISSA)**. IEEE, 2015. p. 1-8. Disponível em: https://ieeexplore.ieee.org/abstract/document/7335054. Acesso em:15 fev. 2021.

COMISSÃO EUROPEIA. Competition policy for the digital era: Final report. Bruxelas, 2019. Disponível em: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>. Acesso em: 21 fev. 2021.

CONDORELLI, Daniele; PADILLA, Jorge. Data-Driven Envelopment with Privacy-Policy Tying, 2020. Disponível em: https://ssrn.com/abstract=3600725 or http://dx.doi.org/10.2139/ssrn.3600725. Acesso em: 16 fev. 2021.

MENDES, Guilherme Adolfo. Simples Nacional: Análise da Constitucionalidade das Exclusões Setoriais. **Conpedi Law Review**, v. 1, n. 8, p. 107-129, 2016.

OCDE. **Relationship between regulators and competition authorities.** 1998. Disponível em : www.ocde.org/dataocde/35/37/1920556.pdf. Acesso em: 16 fev. 2021.

RAUEN, André Tortato. Compras Públicas de inovações segundo o texto final do PL nº 4.253/2020. In: **Nota Técnica nº 80 da Diretoria de Estudos e Políticas Setoriais de Inovação e Infraestrutura (Diset) do Instituto de Pesquisa Econômica Aplicada (IPEA).** Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/nota_tecnica/210209_nt_diset_80_compras_publicas.pdf. Acesso em: 28 fev. 2021.

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

VASCONCELOS, Gabriel. **Nova Lei de Licitações abre caminho para concursos de inovação, diz diretor do Ipea.** Valor Econômico. Disponível em: https://valor.globo.com/brasil/noticia/2021/02/15/nova-lei-de-licitacoes-abre-caminho-para-concursos-de-inovacao-diz-diretor-do-ipea.ghtml. Acesso em: 28 fev. 2021.

(assinado digitalmente)

EDUARDO MOLAN GABAN
DIRETOR PRESIDENTE

(assinado digitalmente)

VINÍCIUS KLEIN
DIRETOR

(assinado digitalmente)

ALUÍSIO DE FREITAS MIELE
DIRETOR

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

(assinado digitalmente)

GABRIEL DE AGUIAR TAJRA
PESQUISADOR

(assinado digitalmente)

JOÃO JOSÉ TURRI BRUFATTO
PESQUISADOR

(assinado digitalmente)

DEBORAH NOVAES
PESQUISADORA

(assinado digitalmente)

ALAÍS APARECIDA BONELLI DA SILVA
PESQUISADORA

Av. Angélica, 879, 6º andar
Higienópolis, São Paulo, CEP 01227-000
www.ibcibr.com.br

Tomada de Subsídios 1/2021

Thamilla Talarico, CIPP/E | Daniel Law [redacted]

seg 01/03/2021 23:38

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

Cc: Jose Eduardo Pieri <pieri@palmaguedes.com.br>; Claudio Roberto Barbosa | Kasznar Leonardos <claudio.barbosa@kasznarleonardos.com>; Erika Diniz <erikadiniz@abpi.org.br>;

1 anexo

Contribuições_ABPI_ANPD.docx;

Boa noite,

Em nome da **ABPI – Associação Brasileira de Propriedade Intelectual**, na qualidade de Coordenadora da Comissão de Estudo de Software, Tecnologia e Proteção de Dados, apresento em anexo a contribuição desta associação na tomada de subsídios sobre a regulamentação da aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, para microempresas e empresas de pequeno porte, bem como iniciav as empresariais de caráter incremental ou disrupv o que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

Atenciosamente,

Daniel Law

Thamilla Talarico, CIPP/E | Daniel Law

[redacted]

daniel-ip.com

Follow us

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: ABPI Associação Brasileira da Propriedade Intelectual

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/** ABPI Associação Brasileira da Propriedade Intelectual
Quais são os desafios/problemas regulatórios relacionados ao tema?	**Um dos principais desafios regulatórios relacionados ao tema é a multiplicidade de realidades institucionais incluídas na classificação de "*microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos*".** **O aspecto desse conceito engloba tanto *startups*, direcionadas para a economia digital – com maior possibilidade de adequação à novas regulamentações, principalmente no que toca à proteção de dados pessoais, bem como empresas de pequeno porte, como comércios locais – padarias, papelarias – para as quais, as demandas decorrentes da adequação regulatória podem implicar na inviabilidade do negócio.**
Existem sugestões para endereçamento do problema?	**A solução para o endereçamento do problema decorre de uma delimitação de cada um dos possíveis agentes abarcados pelo conceito "*agentes de pequeno porte*" e de diferentes regulamentações para cada um deles, em observância com suas realidades e capacidades.**
Quais são as oportunidades relacionadas ao tema?	**O tema pode gerar um maior refinamento na regulamentação relacionada à proteção de dados pessoais no país, a consequência de um menor ônus aos agentes para**

	adequação às normas – especialmente financeiro – tende a ocasionar um maior cumprimento voluntário das regras, e a ampliar a cultura de proteção à privacidade e aos dados pessoais no Brasil.
Quais são as experiências internacionais sobre o tema?	**X**
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	**Natureza dos dados tratados, volume de dados pessoais tratados, receita bruta anual, o tipo de negócio/ ramo de atividade.**
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)?	**Em uma visão geral, pode-se dizer que a União Europeia busca reduzir – na medida do possível – algumas obrigações aos agentes de tratamento de pequeno porte, mantendo a harmonia com a proteção aos titulares de dados. Entendemos que o exemplo mais marcante nesse sentido é a inexistência de uma obrigação generalizada para nomeação de um encarregado – *Data Protection Officer* (DPO) para o GDPR.** **De acordo com a regulação europeia, uma instituição deverá nomear um DPO quando: *(i)* for uma autoridade ou órgão público; *(ii)* suas principais atividade requererem monitoramento em larga escala, regular e sistemático de indivíduos; ou *(iii)* suas principais atividades envolverem o tratamento em grande escala de dados pessoais sensíveis ou dados relacionados a condenações criminais.**
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	**O principal impacto para os agentes de pequeno porte decorrente da manutenção do registro das operações de tratamento de dados pessoais é a necessidade de realização do mapeamento dos dados pessoais tratados e a criação um gerenciamento de fluxo interno, para a atualização contínua do registro.** **A falta de conhecimento sobre o tema e sobre a regulação existente é um grande fator para que essas práticas sejam onerosas a tais agentes, portanto, a realização de campanhas, projetos e cursos pela Autoridade Nacional de Proteção de Dados, visando ampliar o nível de conhecimento sobre privacidade, proteção de dados e a Lei Geral de Proteção de Dados, é um grande impulsionador para a redução dos impactos de tais práticas aos agentes de pequeno porte.**
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	**Os impactos relacionados à nomeação de um encarregado pelos agentes de pequeno porte estão diretamente ligados ao custo financeiro envolvido na contratação e manutenção de um colaborador/ empresa responsável por atuar no cargo em nome da**

	empresa. A depender do modelo de negócio da empresa/ profissional liberal, o volume dados pessoais processados não é compatível com as obrigações e custos decorrentes da manutenção de um colaborador/ ou de uma empresa terceirizada como DPO ocasiona um ônus desarrazoado ao empreendedor. Nesse cenário, a existência de alternativas, como um canal de comunicação para o titular, pode ser razoável para gerar proteção aos titulares de dados e não proporcionar ônus desproporcionais aos agentes.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	**A inexistência de regulação infralegal sobre os critérios e os limites para a elaboração do relatório de impacto à proteção de dados pessoais gera insegurança jurídica e, por vezes, inviabiliza o cumprimento adequado da norma pelos agentes de pequeno porte. Os agentes de pequeno porte, por diversas vezes, não possuem uma equipe jurídica e técnica oferecendo suporte sobre LGPD e devem direcionar recursos para a elaboração do relatório de impacto nos casos que efetivamente ofereçam riscos à proteção de dados pessoais.** **Dessa maneira, a estipulação clara e expressa das circunstâncias nas quais tais agentes devem elaborar o relatório de impacto otimizará seus investimentos na implementação de medidas técnicas e administrativas de proteção de dados pessoais, além de contribuir para um ecossistema efetivo de proteção aos titulares de dados.**
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?	**A necessidade de obtenção de coleta do consentimento do titular ou do responsável para o tratamento de dados pessoais – sensíveis ou de crianças e de adolescentes – bem como todos os direitos decorrentes de tal base legal, pode ocasionar uma complexificação demasiadamente onerosa das práticas administrativas aos agentes de pequeno porte.** **Tendo em vista a relevância da proteção de dados sensíveis e de crianças e de adolescentes, a ANPD pode contribuir com a adoção de regras e/ou modelos simples e não taxativos para formalização de consentimento de forma específica e destacada, para finalidades específicas.**
Quais são os impactos da implementação do programa de	**A implementação de um programa de governança pode acarretar a readequação nos fluxos internos aos agentes de pequeno porte, e por diversas vezes, contratação de consultorias externas. Esse panorama complexifica o modelo de negócios, podendo,**

governança de dados aos agentes de pequeno porte?	**assim, inviabilizar a manutenção do pequeno negócio, caso não haja a estipulação de normas adequadas aos agentes, como a simplificação e a redução das estruturas corporativas necessárias para o atendimento dos pontos necessários para a implementação do programa de governança de dados.**
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	**Os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte estão diretamente relacionados às obrigações regulatórias impostas, que não considerem o volume e a natureza dos dados pessoais tratados pelas empresas de pequeno porte. Portanto, podem ser necessárias relativações e gradações dos níveis de medidas e ferramentas protetivas que cada tipo de agente deve observar.**
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	**A avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte ocasiona – diversas vezes – excessivo ônus financeiro diante do valor de investimento para as ferramentas tecnológicas que realizam a avaliação de risco.**
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	**O impacto da implantação da portabilidade de dados pessoais aos agentes de pequeno porte está diretamente ligado ao custo operacional do cumprimento deste direito. Dessa maneira, é necessário que a regulamentação sobre este direito compreenda em quais modelos de negócio o benefício ao titular prevalece ao ônus ao agente de tratamento, e para quais não há proporcionalidade entre o ônus e o benefício gerado.**
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	**Pode ser elaborado um regime de autorização temporária para que os agentes de pequeno porte sejam autorizados a conduzir seus negócios dentro de um regime regulatório mais flexível, devido ao seu estágio inicial – como no caso das *startups* – ou com base no modelo de negócio desempenhado – como os profissionais liberais ou os pequenos comércios locais.**
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

Tomada de Subsídios 1/2021: Contribuição IBRAC

Sílvia Almeida [redacted]

seg 01/03/2021 21:55

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>; [redacted]

1 anexo

IBRAC_TS_ANPD_Consolidado_01mar2021.pdf;

Prezado(a),

Encaminho, em nome do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (IBRAC), contribuição à Tomada de Subsídios ANDP 1/2021, sobre a regulamentação da aplicação da Lei nº 13.709/2018 para microempresas e empresas de pequeno porte.

Atenciosamente,

Lauro Celidonio
Presidente | IBRAC

Sílvia Fagá de Almeida
Diretora – Mercados Digitais | IBRAC

Thais Cordeiro
Diretora – Relações de Consumo | IBRAC

Ricardo Botelho
Diretor - Regulação | IBRAC

Marcela Mattiuzzo
Coordenadora – GT LGPD | IBRAC

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: **IBRAC – Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional**

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quais são os desafios/problemas regulatórios relacionados ao tema?	Um primeiro grande desafio relacionado ao tema é a **dificuldade de adequação de agentes de pequeno porte às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD).** Em vista da falta de conhecimento e familiaridade de agentes de menor porte sobre regras de proteção de dados, a **adequação de seus negócios à LGPD envolve custos financeiros diversos**, em decorrência da contratação de consultorias jurídicas e tecnológicas, contratação de softwares e tecnologias adequadas, contratação de profissionais especializados em LGPD para exercer o cargo de Encarregado e outros cargos correlatos, e ainda investimentos em monitoramento contínuo de implementação da LGPD de todas as atividades de tratamento de dados e em treinamento de seus profissionais[1]. De acordo com Relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento ("UNCTAD") a respeito do impacto das regulamentações de proteção de dados no comércio[2], a aprovação dessas normas pode colocar empresas de pequeno porte em desvantagem competitiva e criar obstáculos (ônus de compliance regulatório) que poderão incentivar sua saída do mercado, o que, por sua vez, acabaria por desestimular a inovação, reduzir as escolhas do

[1] De acordo com estudo realizado em outubro de 2020 pela consultoria PricewaterhouseCoopers, os custos de adequação à nova lei de proteção de dados variam entre R$50.000,00 (cinquenta mil reais) a R$800.000,00 (oitocentos mil reais). Ademais, conforme estudos presentes em Relatório da OCDE de 2015 (“Emerging Policy Issues: Localisation Barriers to Trade”, disponível em: < https://www.oecd-ilibrary.org/trade/emerging-policy-issues_5js1m6v5qd5j-en >), empresas de pequeno e médio porte que não estão presentes no setor de Tecnologia da Informação e Comunicação (TIC), devem aumentar seus gastos em até 40% com tecnologias para se adequar a regras de proteção de dados rigorosas.

[2] UNCTAD, Data Protection Regulations and International data flows: Implications for Trade Development. 2016. Disponível em: < https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf > Acesso em 18/02/2020

	consumidor e aumentar o risco de monopolização por grandes empresas já estabelecidas no mercado. Como contorno a esses problemas, a flexibilização das normas para esses agentes pode ser considerada uma resposta para garantir a redução dos custos e, assim, não frear a competitividade e inovação no mercado. No entanto, outro desafio surge: **uma flexibilização excessiva de obrigações regulatórias pode também acarretar riscos para a proteção dos direitos de titular de dados, desvirtuando-se das diretrizes da própria LGPD.** Ilustra-se esse problema o fato de existirem agentes econômicos de pequeno porte dedicados à exploração intensiva de dados associados a um número significativo de titulares, que poderiam então, estar sujeitos à uma regulação flexibilizada de forma desproporcional. Sendo assim, é necessário, ao desenhar uma regulação específica aos agentes de pequeno porte, levar em conta um equilíbrio ideal os custos envolvidos para o atendimento de tal regulação e os possíveis problemas para a dinâmica empresarial de diferentes tipos de empresas. A regulação deve ser estruturada de modo que pequenas empresas a vejam como suficientemente legítima e que seus benefícios superem os custos relacionados a seu cumprimento.[3] Ainda, exigências e responsabilidades em face do titular podem variar muito a depender do tipo de agente de pequeno porte e o núcleo de suas atividades, como quando comparamos, por exemplo, um pequeno ponto de venda de bebidas (em que os dados pessoais envolvidos podem consistir apenas nos dos funcionários do local) ou um administrador de banco de dados (o qual pode atuar como operador para grandes empresas que realizam o tratamento de dados sensíveis). **Em vista da diversidade não uniforme de tipos de agentes e suas estruturas com relação ao tratamento de dados pessoais, também surge o desafio da autoridade em desenvolver o endereçamento de uma regulação adequada a cada tipo específico**, de modo que não se desvie da finalidade esculpida pelo art. 55-J, XVIII, da LGPD, que é a criação de uma regulação adaptada às situações em que não seria ideal – e até mesmo prejudicial – aos agentes econômicos previstos no dispositivo a atenderem de maneira inflexível todos os requisitos contidos na LGPD. Outro grande desafio é o de que as **exigências regulatórias cheguem ao conhecimento, de maneira clara e objetiva aos agentes de pequeno porte para que possam entrar em conformidade sem que sejam impedidos pelo desconhecimento de termos técnicos**. Além disso, é preciso considerar também a dificuldade de inserir determinadas práticas com relação à proteção e privacidade de dados dentro do ambiente cultural e rotina dos agentes de pequeno porte. Nesse sentido, para além de uma adequação de uma regulação multisetorial, é necessário um forte trabalho institucional e comunicacional para dispersão de informação e conhecimento afetos ao tema da proteção de dados, de maneira simples, clara e objetiva, modos de adequação e exigências e a

[3] Hatmann Dex. GDPR in Small Business: The Antecedents of Compliance. MSc Business Administration – Small Business and Entrepreneurship (University of Groningen). Faculty of Economics & Business: janeiro, 2019.

	relevância em si da proteção de dados e sua incorporação na empresa, bem como eventuais consequências por não conformidade. Por fim, ainda reside o desafio de **comportar na regulamentação sobre o tema as operações de tratamento de dados relativos ao desempenho de atividade econômica por pessoas físicas e entidades não-empresariais.** Quanto à primeira categoria, ao considerarmos o quadro da economia brasileira, marcada pela informalidade[4], cumulada aos diversos modelos de negócios desenvolvidos por profissionais liberais, o tratamento de dados pessoais por pessoas físicas para fins econômicos passa a ser relevante. Tal constatação também é observada nos casos de entidades não-empresariais, tal como organizações não-governamentais e associações, que podem também realizar atividades de tratamento de dados pessoais em menor ou maior escala. Estes sujeitos, em vista de suas características, também devem enfrentar dificuldades na adequação de seus negócios à LGPD, seja pela falta de recursos financeiros ou pela falta de conhecimento e familiaridade sobre regras de proteção de dados. Da mesma forma que citado anteriormente, algumas exigências podem ser irrazoáveis para garantir a proteção de dados buscada pela lei, em vista das diferentes estruturas de cada agente. Nesse sentido, entendemos que a isonomia de tratamento entre pessoas físicas que manipulam dados para fins econômicos bem como entidades não-empresariais de menor porte, e agentes de pequeno porte, merece ser considerada.
Existem sugestões para endereçamento do problema?	Sim. Uma primeira sugestão, seria garantir que a LGPD seja aplicada, ao menos, de maneira diferenciada e mitigada para esses pequenos empresários e empresas de pequeno porte, ou, mesmo prevendo isenções a essas categorias de empresas e profissionais, de forma a adequar ou mesmo reduzir seu ônus de adequação regulatória. Para regular adequadamente a atuação desses atores, um primeiro passo seria incluir critérios para sua definição como agentes de pequeno porte. Atualmente, empresas de menor porte são classificadas como tal a partir do seu faturamento anual, conforme definição de da Lei Complementar 123/2006. Este critério de definição sozinho para justificar a flexibilização de normas, no entanto, não parece adequado. Como agentes de menor porte podem possuir atividades de tratamento de dados em maior escala e/ou mais arriscadas que agentes de maior porte, a adaptação de normas para agentes a partir de uma classificação baseada em faturamento, poderia implicar em regras desproporcionais para agentes com atividades de tratamento com potencial maior de risco. Nesse sentido, entendemos que a autoridade poderia optar por (i) seguir a definição de micro e pequenas empresas da Lei Complementar 123/2006 e, em seguida (ii) estabelecer critérios secundários, cumulativos, para a definição dos agentes, baseados nas características das atividades de tratamento de dados desempenhadas.

[4] De 38,8%, de acordo com as informações da Pesquisa Nacional por Amostra de Domicílios Contínua do Instituto Brasileiro de Geografia e Estatística (“IBGE”) relativas ao trimestre encerrado em outubro de 2020, citadas em: https://valor.globo.com/brasil/noticia/2020/12/30/desemprego-fica-em-143-atingindo-141-milhoes-de-pessoas.ghtml.

	Ainda, conforme pesquisa realizada em 60 empresas de pequeno porte em diferentes países europeus, em parceria com a União Europeia no âmbito do Programa 2014-2020 de Direitos, Equidade e Cidadania[5], foi possível constatar que os agentes privilegiam a acessibilidade e transparência de autoridades supervisoras no processo de auxílio de adequação dos agentes à regulação, em especial por entenderem que, salvo raras exceções, empresas do mesmo porte não possuem conhecimento interno extensivo sobre o regramento de proteção de dados. Nesse sentido, para que o ônus de adequação de tais agentes não seja demasiado custoso, experiências internacionais apontam para a formulação de guias e orientações públicas, publicadas como manuais, cadernos, panfletos, infográficos, etc., que podem ser inclusive direcionadas a determinados setores, facilitando a compreensão para agentes de determinado ramo. Por meio dessas publicações institucionais é facilitada a difusão de informações em linguagem menos técnica, de modo a facilitar a familiarização com o tema para os agentes e levantar a importância de conformidade com a legislação de proteção de dados. Isso pois a educação relacionada ao tema deve ser feita de tal forma que se reduza a percepção de complexidade, aumente a legitimidade da regulação e denote os custos e consequências envolvidas no seu cumprimento. Dessa forma, também se enquadram nessas sugestões a implementação e difusão de campanhas de conscientização que se mostram relevantes para aumento da capilaridade da regulação. Nesse sentido, podem ser realizadas, além dos mecanismos de consulta pública, a realização de pesquisas específicas sobre o tema para avaliação dos diversos agentes e suas percepções e necessidades ou checagem do nível de conformidade existente. Um ponto importante também é a manutenção de canais de contato com associações, organizações ou entidades representativas de determinados setores de modo a facilitar a abordagem e análise de questões ou problemas existentes e que eventualmente podem decorrer de uma nova regulação e procedimentos. Além disso, poderiam ser oferecidos canais de atendimento (*hot desks*) facilitados e eficientes para o atendimento de dúvidas relacionadas às eventuais exigências diferenciadas pela autoridade em caso de dúvidas. Para temas mais complexos, também poderiam ser previstos mecanismos de consulta administrativa que teriam valor de imunização no que tange à questão e à sugestão decidida. Por fim, como desenvolvido no último tópico de contribuição, a implementação de *sandboxes* regulatórios com a flexibilização das normas em espaços controlados poderia contribuir para promoção de projetos de inovação por empresas de pequeno porte e startups, bem como para adequar dificuldades em detrimento da multiplicidade de setores, com exigências de regulações dinâmicas. Tal instrumento regulatório vem sendo utilizado principalmente em segmentos dos mercados de capitais e financeiro em diversos países. Porém, deve-se ter em conta que é preciso observar os limites legais e de competência para o estabelecimento lícito de sandboxes regulatórias. Outras sugestões importantes nesse sentido, considerando a ideia de flexibilidade e atenuação dos

[5] BARNARD-WILLS, David, et. al. Report on the SME experience of the GDPR. 2019. Disponível em: < https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf > Acesso em 19/02/2021.

	impactos regulatórios sentidos pelos agentes, podem ser a oportunidade de menus regulatórios, com a possibilidade de escolha de regras mandatórias alternativas, e *grandfathering*, consistente em regimes transitórios graduais para as novas estatuídas. Além disso, poderiam ser oferecidos selos e certificações especiais para determinados casos como modo de comprovar conformidade com a lei e regulamentos de modo a aumentar a credibilidade perante terceiros e incentivar a adequação às normas, como prevista na GDPR.
Quais são as oportunidades relacionadas ao tema?	Os ganhos com a regulamentação dos agentes de pequeno porte são diversos. Em primeiro lugar, sua regulamentação, garantindo a adequação de normas para agentes de pequeno porte (originalmente pensadas para grandes processadores de dados), oferece melhores condições para um *level playing field* entre esses agentes e demais empresas. Em segundo lugar, a redução de ônus regulatórios excessivamente onerosos impostos a agentes de pequeno porte contribui para a criação de um ambiente regulatório que fomente a inovação tecnológica, um dos fundamentos da disciplina de proteção de dados inaugurada com a LGPD[6]. Outra oportunidade decorrente da regulamentação do tema é a possibilidade de estabelecer um padrão institucional de relacionamento e comunicação, que poderá facilitar a interação entre os diferentes agentes com a autoridade. Ainda, com uma abordagem adequada da regulamentação, seria possível a difusão de um padrão cultural de maior informação, familiaridade e respeito à temática relacionada a proteção de dados pessoais, principalmente direcionada a agentes que talvez não sejam tão afetos ao assunto. Por esse lado, haveria ao mesmo tempo um incremento na proteção dos direitos dos titulares de dados pessoais e uma imunização de determinados agentes com relação ao revés relacionado às aplicações de sanções relativas ao não cumprimento ou violação da legislação de dados pessoais, como multas que podem significar valores importantes e cruciais para agentes de pequeno porte. Ademais, o tema pode ser aproveitado para o desenvolvimento de relações baseadas na transparência e na proteção de dados pessoais entre clientes, empresas, consumidores e parceiros comerciais. Por fim, o aproveitamento de maior simetria regulatória com experiências internacionais de regulação que já demonstraram sucesso – em especial na União Europeia, que possui legislação similar à brasileira -, garante maior segurança jurídica nas transferências internacionais de dados decorrentes de contratos entre agentes de pequenos portes e fornecedores estrangeiros. De outro lado, o aproveitamento de experiências internacionais também contribui para que a autoridade evite desenhar soluções inadequadas do ponto de vista de políticas públicas de proteção de dados, pela constatação de iniciativas ineficientes desenvolvidas por outras autoridades.

[6] Lei Geral de Proteção de Dados, Art. 2º:
"A disciplina da proteção de dados pessoais tem como fundamentos:
(...) V – o desenvolvimento econômico e tecnológico e a inovação;"

Quais são as experiências internacionais sobre o tema?	Ao observar experiências internacionais sobre o tema, é possível dividi-las em dois níveis: a atuação de países, a partir de sua regulamentação, inclui uma flexibilização total de normas de proteção de dados completa para agentes de pequeno porte, ou, importam em uma flexibilização parcial. No primeiro caso, tem-se regulações que concedem isenções a empresas que estejam abaixo de um determinado limite. A Austrália, por exemplo, a partir do Ato de Privacidade de 1988 ("APA") isenta pequenas empresas e organizações sem fins lucrativos que possuem faturamento anual de $ 3.000.000 (três milhões de dólares australianos) ou menos[7]. Tal isenção, no entanto, não será aplicada para pessoas ou entidades que comercializam informações pessoais, provedores de serviços de saúde, e agências de relatórios de crédito ou agentes que de outra forma lidam com informações financeiras críticas. O APA também oferece um mecanismo de "*opt-in*" para pequenas empresas que receberam essa isenção, para que, voluntariamente, se tornem sujeitas às regras do Ato da mesma forma que uma entidade coberta diretamente pela normativa, com vistas a demonstrar ao mercado e consumidor sua conformidade com o regramento de proteção de dados. Ou seja, seria um mecanismo de adesão voluntária à legislação por aqueles que, mesmo elegíveis à isenção regulatória, veem maiores benefícios na adequação plena de seu negócio ao regime protetivo de privacidade. Além disso, mesmo aceitando voluntariamente a incidência da norma aos seus negócios, esses agentes econômicos podem, posteriormente, notificar sua retirada[8], ampliando o leque de alternativas para lidar com os excessivos ônus regulatórios da legislação de proteção de dados. Da mesma forma, a Lei de Privacidade do Consumidor da Califórnia de 2018 ("CCPA") é aplicável apenas a empresas cuja receita anual exceda US$ 25.000.000,00 (vinte e cinco milhões de dólares americanos), ou cuja metade da receita anual seja obtida com a venda de informações pessoais de consumidores ou que processem informações pessoais de pelo menos 50.000 pessoas anualmente[9]. Vale ressaltar, no entanto, que o último critério é objeto de diversas críticas por implicar em limiar demasiado baixo - e por consequência ampliar o universo de empresas sujeitas ao regime protetivo - visto que é razoavelmente fácil atingir o patamar de 50.000 pessoas/ano[10]. Nesse critério baseado em volume de dados ou titulares potencialmente afetados, o Japão, por exemplo, optou por abandonar a isenção conferida a entidades que não tratam informações pessoais de mais de 5.000 indivíduos em qualquer dia nos últimos seis meses. Cumpre mencionar, porém, que a legislação de proteção de dados japonesa permite que isenções sejam fornecidas em uma análise

[7] AUSTRALIA, Privacy Act. 1988. Seção 6D. Disponível em: < https://www.legislation.gov.au/Series/C2004A03712 > Acesso em 18/02/2021.
[8] *Ibid*. Seção 6EA.
[9] ESTADOS UNIDOS DA AMÉRICA, California Consumer Privacy Act. 2018. Seções 1798.100 a 1798.199 e Seção 1798.140(c). Disponível em: < https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121&showamends=false > Acesso em 18/02/2021.
[10] Ver: COMSTOCK, Brendon. How the CCPA could be great for startups. 2018. Disponível em: < https://iapp.org/news/a/how-the-ccpa-could-be-great-for-startups/ > Acesso em 18/02/2021.

	casuística, por meio de decisões nos casos em que o risco de danos aos direitos e interesses dos indivíduos se mostre limitado[11]. Do outro lado, o Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") recomenda que os Estados membros levem em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do regulamento[12], se aproximando de um modelo por isenções parciais. Em primeiro lugar, o GDPR isenta empresas com menos de 250 funcionários da obrigação de manutenção de registros de atividade de tratamento de dados, contanto que o tratamento de dados não seja ocasional, não resulte em riscos à liberdade de indivíduos e/ou não envolva determinadas categorias como dados pessoais sensíveis ou condenação criminal. além de trazer exceções à obrigação de nomeação de *Data Protection Officer* ("DPO"), cuja figura equivalente na legislação brasileira seria o Encarregado. Vale ressaltar que, a implementação de exceções e flexibilizações normativas para agentes de menor porte em regramentos de proteção de dados pessoais não necessariamente reduzirá a dificuldade de adequação pelos agentes. No caso da União Europeia, segundo pesquisa[13] realizada pelo GDPR.EU, os principais pontos problemáticos relacionados à adequação das pequenas empresas[14] na Espanha, Reino Unido, França e Irlanda ao GDPR são: (i) aproximadamente metade das empresas estavam falhando em cumprir requisitos essenciais de linguagem clara sobre o tratamento aos titulares e identificação de base legal; (ii) confusão com conceitos básicos de segurança de dados; (iii) realização de investimentos em tecnologia e consultas para adequação; e (iv) reconhecimento majoritário da importância de conformidade à legislação. De forma mais geral, foi observado[15] que as principais impressões de pequenas empresas na União Europeia no que tange à adaptação legal foram: custos consideráveis para adaptação, dificuldade no atendimento de direitos dos titulares em razão da falta de ferramentas adequadas, relativa dificuldade na implementação do princípio de prestação de contas pelo aumento de recursos humanos e custos financeiros, falta de derrogações adequadas a esse tipo empresarial, importância dos códigos de condutas para cumprimento da legislação, elevados custos relativos à certificação, reconhecimento do valor de guias e ferramentas práticas disponibilizadas, fardo com aumento da documentação, alto

[11] JAPÃO, Ato de Proteção de Dados Pessoais, Artigo 2º, Capítulo IV, Seção 1. Disponível em: < https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf > Acesso em 18/02/2021.
[12] UNIÃO EUROPEIA, General Data Protection Regulation, Recital (98), (132) e (167); Seção 5, Artigo 40. Disponível em: < https://gdpr-info.eu/ > Acesso em 18/02/2021.
[13] 2019 GDPR Small Business Survey. Disponível em: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf
[14] A definição da pesquisa é a de que pequenas empresas possuem menos de 500 empregados. Entretanto a categoria legislativa europeia de define como médias-empresas até 250 pessoas, considerando o enquadramento econômico. De qualquer modo consideramos possível extrapolar, ainda que grosseiramente, o resultado da pesquisa para agentes de pequeno porte.
[15] Contribution From The Multistakeholder Expert Group To The Stock-Taking Exercise Of June 2019 On One Year Of Gdpr Application. 13 junho de2019. Disponível em: https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf

	custos na elaboração relatório de impactos a proteção de dados pessoais, diminuição de custos de transação a partir de cláusulas contratuais padrão. Nesse sentido, algumas autoridades nacionais buscam remediar essas dificuldades oferecendo guias e suporte prático de orientação e adequação à legislação de proteção de dados, nesse sentido se destacando a autoridade francesa[16], a autoridade irlandesa[17] e autoridade do Reino Unido[18]. Além disso, são também praticadas campanhas de conscientização voltadas a pequenas empresas para que tomem conhecimento sobre a legislação de proteção de dados e auxiliar esses agentes no cumprimento de suas obrigações legais[19]. Dessa forma, as autoridades vêm prezando pela conscientização e facilitação às pequenas empresas por meio de guias, ferramentas (como contratos padrões e registros de atividades), FAQs, canais de atendimento, campanhas e linhas de apoio. A União Europeia, de forma centralizada a partir do sítio ec.europa.du, também já publicou informativos para auxiliar pequenas empresas na adequação ao GDPR[20]. No Reino Unido, por exemplo, o *Information Commisioner's Office* (ICO) visualiza a possibilidade de realização de um *sandbox* regulatória para casos de tratamento de dados pessoais, realizando uma consulta pública para visualização das dificuldades para inovação relacionadas ao tema da proteção de dados, qual seria o escopo de aplicação da *sandbox* regulatória, seus benefícios e mecanismos de funcionamento.[21] Em geral, houve um feedback positivo para o desenvolvimento de tal instrumento regulatório, mas a autoridade consignou que este deveria estar limitado a produtos e serviços que representem inovação genuína, que demonstrem benefícios materiais aos titulares de dados e que possuem uma estrutura de prestação de contas robusta para o tratamento de dados pessoais. Por fim, vale ressaltar ainda a dificuldade observada em experiências internacionais quanto à convergência de regulamentos setoriais com regras de proteção de dados. A exemplo, no setor agrícola, perspectivas antagônicas às premissas do GDPR foram adotadas na União Europeia para o tratamento de determinadas informações do setor agrícola (e de outros setores econômicos) com a edição do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia[22] .

[16] Guia disponível em: https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.
[17] Guia e orientação disponíveis em: https://www.dataprotection.ie/en/dpc-guidance/guidance-smes
[18] Em seu site, a ICO disponibiliza uma série de informações, orientações e ferramentas para pequenas empresas com relação à proteção de dados pessoais: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/
[19] GDPRights: GDPR awareness campaign and support to business organisations, in particular, SMEs. Disponível em: https://idpc.org.mt/idpc-publications/gdpr-awareness-campaign-business-organisations-in-particular-smes/https://idpc.org.mt/idpc-publications/gdpr-awareness-campaign-business-organisations-in-particular-smes/
[20] Documento disponível em: https://ec.europa.eu/justice/smedataprotect/index_en.htm.
[21] O resumo da análise dos comentários da ICO está disponível em: https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf
[22] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1807.

Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Partindo de disposições já existentes no ordenamento jurídico brasileiro (Lei Complementar nº 123/2006, art. 1º, §§ 3º e 6º; Constituição Federal, arts. 146, "d", 170, IX, e 179; Lei nº 13.874/2019, art. 4º), nota-se que há autorização legal para criação de regimes especiais simplificados para microempresas e empresas de pequeno porte. Há, também, definições de "startups", "microempresas" e "empresas de pequeno porte" em normas vigentes ou avançadas no processo legislativo que podem ser consideradas pela autoridade, com o objetivo de uniformização do ordenamento jurídico e garantia de segurança jurídica na aplicação das normas. Não obstante, a definição de um *proxy* preciso para definição de agentes de pequeno encontra dificuldades tanto em termos quantitativos quanto em termos qualitativos, pois deve considerar os diferentes tipos de agentes envolvidos, suas intersecções e os riscos relacionados. A utilização apenas de fatores quantitativos (como número de funcionários, receita anual, valor dos ativos, volume de dados) pode ser um problema, pois esses números podem muitas vezes não refletir os riscos aos direitos dos titulares e suas possíveis violações. Ademais, a consideração de valores qualitativos pode trazer problemas de enquadramento de determinados agentes como agentes de pequeno porte quando em comparação com critérios quantitativos mais objetivos, além de que apesar de endereçarem as questões de risco de modo mais adequado, podem não refletir o risco factual na realidade de determinado a gente quando levada de maneira isolada. Assim, os critérios devem ser conjugados de modo a trazer uma definição mais correta de agentes de pequeno porte. Nesse sentido, experiências internacionais podem contribuir para a definição de critérios que se mostrem mais razoáveis para um ideal equilíbrio entre os fundamentos da disciplina de proteção de dados previstos na LGPD. A União Europeia, por exemplo, utiliza como critério para necessidade de designação de Encarregado a (i) existência de tratamento de dados como parte de atividades essenciais e não auxiliares da empresa e (ii) a existência de tratamento em larga escala. Similarmente fez a autoridade de proteção de dados australiana, que isenta da aplicação de obrigações de sua legislação de proteção de dados pequenas empresas com base no seu faturamento, ainda que tal isenção não seja aplicada para agentes que comercializam informações pessoais, sejam provedores de serviços de saúde, ou sejam agências de relatórios de crédito ou agentes que de outra forma lidem com informações financeiras críticas. Em suma, entendemos que a ANPD poderia se valer dos critérios já estabelecidos em leis existentes ou em discussão legislativa no Brasil como ponto de partida para a definição de agentes de pequeno porte, garantindo, contudo, flexibilização e adaptação de obrigações para aqueles que se enquadrarem na classificação da lei, ainda que, permita exceções para a classificação dos agentes, a depender da vulnerabilidade dos dados tratados em suas atividades de tratamento, o volume de dados tratados, a existência de atividades de tratamento essenciais ao negócio, entre outros critérios secundários.

	Vale pontuar que o conceito de agentes de tratamento de dados de pequeno porte deve abranger as pessoas físicas que desempenham atividades econômicas de maneira desvinculada de pessoas jurídicas. Ademais, entendemos ser recomendável a criação de dois "blocos" de definição e regulamentação específica: PMEs, pessoas físicas e microempresas, de um lado, e startups, de outro, a fim de que sejam respeitadas as particularidades desta figura.
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)?	Para além das regras de isenção parcial prescritas no GDPR, a União Europeia divulga material informativo prático para auxiliar e conscientizar pequenas empresas sobre a importância de adaptação às novas regras legais existentes.[23-24] Além disso, há incentivos a campanhas de conscientização e ações de sensibilização nos níveis europeu e nacional através do financiamento, podendo ser citadas as experiências nacionais de campanhas de conscientização da Bélgica, Dinamarca, Holanda, Eslovênia, Islândia, Letônia, bem como a criação de ferramenta inovadora para pequenas empresas da Bulgária e materiais de treinamento direcionados a esse perfil pela Hungria.[25] Como ações futuras dentro desse tema, o bloco europeu ainda prevê "desenvolver instrumentos práticos, tais como formulários harmonizados para as violações de dados e os registros simplificados das atividades de tratamento, para ajudar as PME de baixo risco a cumprirem as suas obrigações" e "apoiar as atividades das autoridades de proteção de dados que facilitem a aplicação das obrigações decorrentes do RGPD pelas PME, através de apoio financeiro, especialmente para orientações práticas e ferramentas digitais que possam ser reproduzidas noutros Estados-Membros".[26] Vale notar que a Agência de Cibersegurança da União Europeia (ENISA), já se manifestou preocupada com a adequação de empresas de pequeno e médio porte, ao publicar Guia de Segurança em Sistemas de Computação em Nuvem para Empresas de Pequeno e Médio Porte[27] e Guias sobre Segurança em Tratamento de Dados Pessoais por Empresas de Pequeno e Médio Porte[28], recursos estes, importantes para atender a requerimentos técnicos de segurança exigidos pelo GDPR. Ainda, com base em levantamento feito em setembro de 2020 por projeto de pesquisa da União Europeia no âmbito do Programa 2014-2020 de Direitos, Equidade e Cidadania[29], pouco menos de um terço das autoridades de proteção de dados europeias oferecem orientações direcionadas

[23] Seven steps for businesses to get ready for the General Data Protection. Disponível em: https://ec.europa.eu/info/sites/info/files/gdpr2019-smes_7_steps_brochure-en-v03_lr_qc.pdf
[24] Better rules for small business. Disponível em: https://ec.europa.eu/justice/smedataprotect/index_en.htm
[25] Informação e mais detalhes disponíveis em: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en
[26] Comissão Europeia. Comunicação (2020), 264: A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital - dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0264&from=EN#footnoteref49.
[27] Disponível em: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes
[28] Disponíveis em: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/march-2015/presentations/presentation-nlos-cgm-v2.pdf e https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.
[29] JASMONTAITĖ-ZANIEWICZ, Lina et al. The GDPR made simple(r) for SMEs. 2021. p. 24. Disponível em: <https://library.oapen.org/bitstream/handle/20.500.12657/46614/Handboek_GDPR_ENG_HR-cert-febr4.pdf?sequence=1> Acesso em 16/02/2021.

	especificamente para empresas de pequeno e médio porte. Daquelas que realizam, vale ressaltar, principalmente, a atuação das autoridades nacionais inglesa, ICO, (até início de 2020, pertencente à UE) e eslovena, IP. Quanto à autoridade inglesa, medida interessante implementada pela entidade foi segmentar o atendimento a empresas de menor porte em relação àquelas de grande porte, a partir de um canal telefônico específico para atender às dúvidas e demandas de pequenas empresas. Em sua plataforma online, a autoridade também disponibiliza FAQs, checklists para avaliar grau de adequação ao GDPR, templates para políticas de privacidade, to-do lists para respostas de incidentes de segurança, entre outros instrumentos em linguagem facilitada e direta para facilitar o atendimento do GDPR por agentes de pequeno porte[30]. A autoridade eslovena, por sua vez, possui uma plataforma específica direcionada somente a empresas de pequeno e médio porte, onde estas podem acessar FAQs e formulários para designação de encarregado, para notificação de incidentes à autoridade, para notificar titulares sobre a obtenção de seus dados, bem como formulários para registro de atividades de tratamento de dados (adaptadas para controladores e operadores), em atenção à exigência de registro de atividades de tratamento prevista no GDPR (Art. 30)[31]. A autoridade também ofereceu um canal telefônico de auxílio a empresas de pequeno e médio porte durante um ano após a entrada em vigor do GDPR. Demais autoridades também apresentam iniciativas destinadas a auxiliar empresas de pequeno porte. A autoridade belga (APD), também possui guias de adequação ao GDPR, FAQs e campanhas de conscientização destinadas a agentes de pequeno e médio porte. A autoridade francesa[32] (CNIL) e a lituana[33] (VDAI) também possuem guias com linguagem simplificada para adequação ao GDPR de empresas de micro, pequena e médio porte. No mesmo sentido, a autoridade irlandesa também dispõe em sua plataforma online guia de adequação destinado a empresas de pequeno e médio porte, incluindo checklists de adequação e templates para mapeamento de atividades de tratamento atuais das empresas[34]. A autoridade espanhola (AEPD), por sua vez, conta com ferramenta em sua plataforma online destinada a auxiliar a adequação de empresas que realizam tratamento de dados pessoais que implicam em riscos menores (que podem abranger o caso de diversos agentes de pequeno porte), conforme seu setor de atuação[35]. Por fim, há expectativa de se tornar a linguagem acessível, prática e menos técnica, garantindo que os agentes possam entender as orientações com menor dificuldade[36]. E em caso de infração às normas de proteção de dados, a União Europeia adota uma linha de imposição gradual de

[30] Disponível em: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/
[31] Disponível em: https://upravljavec.si/vprasalnik/
[32] Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf
[33] Disponível em: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_SVV_BDAR_2018.pdf
[34] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf
[35] Disponível em: https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd
[36] BARNARD-WILLS, David, et. al. Report on the SME experience of the GDPR. 2019. p. 31 Disponível em: <https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf> Acesso em 19/02/2021.

	penalidades. Inicialmente é feito um aviso, seguido de advertência, suspensão e, em casos mais graves, até mesmo multas de até 20 milhões de euros ou 4% da receita anual global.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	A depender da organização, a manutenção de registro das operações de tratamento de dados pode representar um custo elevado, tanto financeiro quanto administrativo. A título de exemplo, volumes excessivos de dados podem aumentar os custos de armazenagem de informação. A experiência europeia, nesse sentido, aponta para esse relevante impacto e para a dificuldade de adequação à GDPR por pequenos empresários e empresas de pequeno porte[37]. Contudo, o registro de operações de tratamento de dados pessoais auxilia no cumprimento da transparência e da prestação de contas perante terceiros e autoridades. Resumidamente, trata-se de um mecanismo importante para apoiar uma análise de riscos de qualquer atividade de tratamento existente em uma empresa. Sua manutenção facilita a avaliação factual do risco das atividades de tratamento realizadas por um controlador ou operador sobre os direitos dos indivíduos, e a identificação e implementação de medidas de segurança adequadas para salvaguardar os dados pessoais - ambos componentes essenciais do princípio de responsabilidade contido na LGPD. Por esse motivo, um modelo mais flexível, como o desenvolvido pela GDPR, pode ser mais adequado para agentes de pequeno porte que não representem riscos demasiados a direitos dos titulares. Atualmente, a LGPD estabelece que o registro é obrigatório para todas as atividades de tratamento, não possuindo exceções, seja para categorias de agentes sujeitos à norma, seja para atividades específicas de tratamento. Ademais, a lei não prescreve modelo de registro que possa ser implementado pelas empresas com segurança, as quais correm o risco de receber questionamento por omissões em registros pela autoridade nacional no futuro, em vista da falta de orientação. Desta forma, em linha com o entendimento do *Working Party* 29 sobre o registro de atividades de tratamento por empresas de micro, pequeno e médio porte[38], recomenda-se que a ANPD forneça ferramentas para facilitar a criação e gestão de registro. Por exemplo, poderia ser disponibilizado no sítio da ANPD na Internet, um modelo simplificado que pode ser utilizado pelos agentes para manter registros das atividades. Ademais, a autoridade poderia estabelecer um prazo de armazenagem de dados diferenciado para empresas de menor porte, bem como se valer de derrogações implementadas pela União Europeia em relação à obrigação de registro de atividades de tratamento prevista no GDPR. Conforme o art. 30 do Regulamento europeu, o registro de atividades de tratamento por empresas ou organizações que empreguem menos de 250 pessoas pode ser dispensado, a não ser que o tratamento de dados conduzido pela pessoa jurídica possa resultar em risco aos direitos e liberdades de titulares de dados,

[37] Ver: https://gdpr.eu/2019-small-business-survey/ e https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf.
[38] WORKING PARTY 29, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR. Disponível em: <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422> Acesso em 18/02/2021.

	seja ocasional ou o tratamento inclua dados sensíveis ou dados relacionados a ofensas e condenações criminais. Entendemos que exceções similares poderiam ser implementadas para agentes de pequeno porte no Brasil.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Entre os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte está o alto custo a ser despendido neste trâmite. Vale lembrar, os agentes de pequeno porte não possuem tantos recursos para realizar tal nomeação. Desta forma, seria relevante o aproveitamento dos critérios presentes na GDPR sobre a flexibilização da exigência de encarregado para os agentes de pequeno porte. Na GDPR, a designação de encarregado é dispensada para os agentes de pequeno porte, caso o tratamento de dados não seja feito em larga escala. Além disso, a União Europeia recomenda a nomeação de encarregado para os agentes de pequeno porte nos casos em que: (i) se processe dados pessoais para direcionar publicidade, através de motores de busca com base no comportamento online dos indivíduos e (ii) se processe dados relacionados a genética e saúde para hospitais. Estas sugestões podem ser encontradas no seguinte link: https://ec.europa.eu/justice/smedataprotect/index_en.htm Além disso, cumpre destacar que, assim como agentes empresariais de pequeno porte, outras pessoas físicas e entidades não empresariais, como ONGs, podem enfrentar dificuldades semelhantes. Portanto, seria importante uma flexibilização também em relação a estes entes. Para a designação de Encarregado, a União Europeia criou exceções para empresas que não tem o tratamento de dados como parte de suas atividades essenciais, isto é, as atividades primárias das empresas (Recital 97, GDPR). Ainda, a designação de Encarregado pode ser dispensada para empresas que não realizam o tratamento de dados em larga escala, isto é, operação em grande escala com objetivo de tratar uma quantidade considerável de dados pessoais em nível regional, nacional ou supranacional que poderia afetar número grande de titulares de dados, e que poderiam acarretar possivelmente em alto risco (Recital 91, GDPR). Outros critérios para definir se um tratamento é realizado em larga escala, de acordo com o *Working Party* 29, é avaliar: (i) o número de titulares de dados sujeitos ao tratamento (número determinado ou proporção de uma população relevante); (ii) volume dos dados ou o leque de diversidade de dados sendo tratados; (iii) a duração ou permanência da atividade de tratamento; (iii) a extensão geográfica da atividade de tratamento[39].

[39] De acordo com o Working Party 29, conforme os critérios apresentados, são considerados tratamentos de larga escala: (i) tratamento de dados do paciente no curso normal dos negócios por um hospital; (ii) tratamento de dados de viagem de indivíduos usando o sistema de transporte público de uma cidade (por exemplo, rastreamento por meio de cartões de viagem); (iii) tratamento de dados de geolocalização em tempo real de clientes de uma rede internacional de fast food para fins estatísticos por um operador especializado na prestação desses serviços; (iv) tratamento de dados de clientes no curso normal dos negócios por uma seguradora ou banco; (v) tratamento de dados pessoais para publicidade comportamental por um mecanismo de pesquisa; e (vi) tratamento de dados (conteúdo, tráfego, localização) por telefone ou provedores de serviços de internet.

	Estabelece também o *Working Party* 29[40] que o tratamento de dados por pessoas físicas (como de um paciente por um médico ou de condenações e ofensas criminais por um advogado), logo, não abrangem tratamento de larga escala, de forma que a designação de DPO, neste caso, poderia ser dispensada. A mesma conclusão se aplica a diversas empresas de pequeno porte e microempresas, que possuem volume de dados, número de titulares, duração e extensão geográfica do tratamento reduzida. Assim, entendemos que estes critérios poderiam ser aproveitados pela Autoridade para dispensar a exigências de nomeação de Encarregado para agentes de pequeno porte. Ainda, vale ressaltar que, muito embora a LGPD exija a indicação de DPO, a lei não deixa claro se o Encarregado poderá exercer a mesma função para outras empresas (isto é, se uma mesma controladora poderá compartilhar um Encarregado com outras controladoras). Tal possibilidade é prevista em normativa europeia, de forma que duas ou mais controladoras possam contratar um mesmo Encarregado, contanto que ele seja facilmente acessível e possa seguir com seu papel individualmente sem conflito de interesses entre as empresas. A terceirização de DPO, neste formato, pode importar em uma redução de custos comparada à contração de um DPO exclusivo para o agente. Assim, entendemos que a Autoridade poderia esclarecer essa possibilidade a partir de regulamentação futura, facilitando a gestão de recursos de agentes de pequeno porte na adequação à LGPD.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	O relatório de impacto é um relevante instrumento de mitigação de riscos e eventuais problemas relacionados à violação dos direitos dos titulares, de forma que, ao reduzir riscos, há possivelmente uma diminuição de custos e futuras despesas, além de se possibilitar a detecção de falhas. Por outro lado, a elaboração de um relatório de impacto também pode representar custos elevados para os agentes de menor porte. Desta forma, sugere-se que haja uma flexibilização quanto aos critérios e modelos de relatório, para que se tornem mais simples ou mais completos a depender da especialidade do setor. Assim, atividades relacionadas a questões de saúde, por exemplo, podem demandar um relatório mais completo. Portanto, seria importante que a ANPD determinasse modelos mais simples ou mais completos a serem adotados para setores específicos, à medida da necessidade dos riscos envolvidos.
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?	Em decorrência da sensibilidade do tema, o tratamento destes dados pode resultar em custos mais elevados aos agentes de pequeno porte. Portanto, seria pertinente o fornecimento, pela ANPD, de orientações mais específicas sobre como se adequar aos regulamentos, transmitidas de forma coesa e didática.

[40] WORKING PARTY 29, Guidelines on Data Protection Officers (“DPOs”), 2017. Disponível em: < https://ec.europa.eu/newsroom/document.cfm?doc_id=44100 > Acesso em 18/02/2021.

	Vale ressaltar, a flexibilização, para agentes de pequeno, do regulamento referente ao tratamento dos dados em questão é extremamente sensível, à medida em que exigem uma maior cautela e proteção. Caso fosse feita a flexibilização, seria interessante que se utilizasse, assim como sugerido em outros pontos, o critério de setores de atividade, com modelos mais simplificados ou mais completos, a ser determinado pela ANPD. Ademais, seria pertinente que a autoridade orientasse de forma clara como garantir e autenticar o consentimento do tratamento e coleta destes dados. Quanto aos dados de crianças e adolescentes, a cautela no seu tratamento se justifica pela vulnerabilidade da situação dos titulares em questão, presumido que estão menos cientes dos riscos do tratamento de seus dados para finalidades que possam não ser adequadas, e que, em vista de sua capacidade jurídica reduzida, não respondem por decisões tomadas quanto ao tratamento de seus dados (a exemplo, ao consentirem com o tratamento de seus dados). Por fim, é relevante ressaltar a necessidade de um posicionamento mais contundente por parte da autoridade sobre as demais bases legais aplicáveis aos dados de crianças e adolescentes.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Um programa de governança de dados deve ser entendido como parte de uma lógica de governança mais ampla, que abrange boas práticas para a elaboração de políticas internas, planos de resposta a incidentes, mecanismos de supervisão internos e análise de riscos em geral. Trata-se de um arcabouço de práticas que não pertence à realidade empresarial da esmagadora maioria dos agentes econômicos de pequeno porte no Brasil. Exigir a implementação de uma política de governança de dados para pequenas empresas, portanto, significaria impor gastos desproporcionais para esses negócios. Não se menosprezam aqui, evidentemente, as consequências positivas que tais programas poderiam ter para essas empresas, que no longo prazo acabariam mesmo por se valorizar, ao estabelecer uma maior relação de transparência e confiança com os titulares de dados e mitigar eventuais prejuízos futuros com a violação de direitos nessa seara. Contudo, dada a realidade dos pequenos negócios no Brasil e a delicada conjuntura econômica que ainda reflete os efeitos da pandemia, seria essencial que fossem flexibilizados os requisitos para a implementação de um programa de governança de dados para as pequenas empresas. Também seria importante que a ANPD atuasse de forma pedagógica quanto a essa exigência, fornecendo guias práticos para sua implementação, bem como *templates* de procedimentos, políticas, notificações e demais instrumentos que compõem tais programas, como fazem as autoridades europeias.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Primeiramente, é importante destacar que não existe no texto da LGPD uma definição mais ampla quanto a quais serão os requisitos que a ANPD implementará em matéria de segurança de dados pessoais. Justamente por isso, o assunto é objeto de uma outra Tomada de Subsídios, iniciada

	recentemente pela Autoridade[41]. Diante dessa ausência momentânea de regras em caráter geral, há naturais dificuldades de vislumbrar exatamente como seriam os requisitos específicos exigidos dos agentes econômicos de pequeno porte. Dito isso, a implementação de políticas de segurança relativa à proteção de dados pessoais eleva as práticas técnicas e organizacionais de empresas, exigindo um maior compromisso de funcionários na gestão de informações pessoais. Atualmente, a maioria dos agentes de pequeno porte não dispõem de medidas adequadas que garantam a segurança da informação de forma sofisticada. Empresas de menor porte ainda possuem reduzidas salvaguardas de segurança da informação, muito distantes das melhores práticas das grandes organizações, que investem vultosos recursos nesse tipo de proteção. Como é sabido, os custos de sistemas como esses são extremamente relevantes e, portanto, fora da realidade de boa parte das pequenas empresas. Dessa forma, a política de segurança relativa à proteção de dados pessoais nos agentes de pequeno porte deve ser mais bem direcionada a suas peculiaridades, de forma a preencher a lacuna entre as disposições legais e sua compreensão e percepção de riscos à segurança da informação. Na prática, esta orientação deve vista como um guia de entrada que permita a esses agentes relacionar adequadamente suas atividades de tratamento com as disposições legais, de forma que possam identificar as medidas de segurança relevantes que devem implantar.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	Como comentado na questão sobre o programa de governança, acima, a avaliação sistemática de riscos não faz parte da realidade empresarial da maior parte dos agentes econômicos de pequeno porte, posto que implica implementar uma vasta gama de práticas, que inclui o mapeamento de atividades de tratamento de dados, matrizes de riscos conforme atividades e planos de ação para adequação à LGPD. Cada uma dessas etapas exige dos agentes conhecimento das complexidades e peculiaridades da legislação, tais como as definições específicas da lei, sua abrangência e exceções à aplicação, bases legais e condições de transferência internacional de dados, entre outros requisitos específicos. Dessa forma, a condução de uma avaliação sistemática de riscos é demasiadamente custosa às empresas, seja quando essa atividade é terceirizada a partir de consultorias técnicas e jurídicas, seja pela conscientização de funcionários a partir de workshops, treinamentos e implementação de políticas internas. A exigência de uma avaliação de riscos, portanto, deveria ser flexibilizada para as pequenas empresas no que for possível, talvez segregando os agentes de pequeno porte pelo volume e/ou tipo de dados com que lidam, e a partir disso estabelecendo obrigações mais condizentes com sua prática. Paralelamente a isso, e em linha com as experiências internacionais, entendemos que a autoridade nacional poderia envidar esforços para elaborar guias práticos, em linguagem facilitada para a

[41] Tomada de Subsídios 2/2021, publicada no dia 22/02/2021, conforme Notícia no site da ANPD: https://bit.ly/3pUG7ue

	implantação de processos que compõem a avaliação sistemática de riscos à privacidade, além de oferecer *templates* de documentos (matrizes de riscos, inventários de dados etc.) que possam ser preenchidos com mais facilidade pelos agentes de pequeno porte.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Inicialmente é importante que a Autoridade defina as exigências regulatórias de modo claro e objetivo, de modo que as pessoas físicas e empresas, especialmente de pequeno porte, possam entrar em conformidade sem entraves desnecessários. Conforme destacado anteriormente, o custo de entendimento das exigências regulatórias pode se mostrar demasiadamente custosa às empresas caso não sejam definidas regras claras. Embora o direito de portabilidade de dados deve seguir diretrizes ainda não regulamentadas pela autoridade nacional (Art. 18, V, LGPD), a garantia desse direito implica no investimento de recursos tecnológicos específicos e treinamento de funcionários que podem significar custos elevados para agentes de pequeno porte. São custos financeiros relacionados à gestão e criação de processos que envolvem localização e identificação de dados dos titulares e sua padronização em um espaço de tempo adequado e razoável. Os agentes de pequeno porte teriam também de criar canais e processo aptos a atender de maneira eficaz e adequada os pedidos de portabilidade de dados pessoais, podendo impor dificuldades operacionais consideráveis. Vale ressaltar, que, conforme o entendimento da autoridade inglesa de proteção de dados pessoais, uma “taxa razoável” pelos custos administrativos do cumprimento da solicitação poderia ser cobrada do titular solicitante, caso a solicitação seja manifestamente infundada ou excessiva. A implementação dessa taxa poderia ser amparada por regulamentação da ANPD para agentes de pequeno porte, o que facilitaria o atendimento ao direito de portabilidade por pequenas empresas. Ainda, deve-se mencionar que, conforme mandamento do Art. 40 da LGPD, poderá a ANPD dispor sobre padrões de interoperabilidade para fins de portabilidade. Uma sugestão, portanto, seria oferecer padrões de interoperabilidade mínimos pelos quais empresas de pequeno porte poderiam se guiar. Adicionalmente, soluções podem surgir dentro do próprio mercado para facilitar aos agentes de pequenos realização da portabilidade de dados pessoais. A exigência de portabilidade pode disseminar práticas de padronização e estruturas de compartilhamento de dados entre os próprios agentes, facilitando sua interação. Apesar dos custos e desafios mencionados, é reconhecido que a portabilidade de dados é fundamental para aumentar a concorrência em setores que dependam da utilização de dados pessoais. A definição regras claras para o tratamento de dados e para a migração de dados significa aumento da competitividade nesses mercados, com impactos positivos sobre o bem-estar do consumidor, entre outros benefícios.

Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	Entendemos que o uso de *sandboxes* regulatórios poderiam ser implementados pela Autoridade para promover a inovação em agentes de pequeno porte. Como antecipado, o uso de *sandboxes* regulatórios permite que, em espaços experimentais, empresas e seus modelos de negócios inovadores que não se encaixem totalmente no arcabouço regulatório vigente possam operar em caráter temporário. Isto pode ocorrer desde que atendidas algumas condicionantes que podem limitar aspectos como, por exemplo, o número de usuários, a prestação do serviço em uma área geográfica limitada ou o período no qual o produto pode ser oferecido no mercado. O uso de *sandboxes* regulatórios já tem sido prática recorrente internacional nos setores financeiro e, mais recentemente, tem sido incorporado no setor regulado de telecomunicações. Sobre este último, vale ressaltar que a Agência Nacional de Telecomunicações (ANATEL), não só tem mantido recorrente troca de conhecimento com agências estrangeiras a respeito da implementação de *sandboxes* no setor regulado (como a agência colombiana de telecomunicações), como em 2020, a partir da Consulta Pública nº 65, recolheu subsídios de empresas do setor sobre a possibilidade de reforma regulatória que incluísse entre seus principais pontos, a inclusão de modelos de *sandboxes* regulatórios. Em matéria de privacidade e proteção de dados, a autoridade nacional inglesa de proteção de dados, ICO, já implementou, em 2018, modelo de *sandbox* regulatório que permitia a empresas com modelos de negócios inovadores contassem com o apoio, a orientação e supervisão da autoridade. Dessa forma, entendemos que a ANPD poderia valer-se da flexibilização de algumas normas para startups e agentes de pequeno porte para garantir o desenvolvimento de seus projetos inovadores, mesmo observando princípios e diretrizes de proteção de dados e segurança da informação. Inclusive, em se tratando de proteção de dados pessoais e privacidade, entendemos que a flexibilização de regras condicionada à operação de empresas em espaço, tempo e com número de usuários limitados e com a supervisão da Autoridade, reduziria os riscos de violações de dados e, em caso de um incidente de segurança, favoreceriam a adoção, de forma mais assertiva, de medidas técnicas para suprir eventuais danos causados[42]. Vale ressaltar que os *sandboxes* também podem contribuir para a facilitação de financiamento de modelos de negócio inovadores, sendo mais um atrativo à sua implementação. De acordo com relatório da Autoridade de Condutas Financeiras do Reino Unido (FCA), 40% das empresas que participaram do *sandbox* inaugural para serviços financeiros em 2017 receberam investimento durante

[42] As experiências internacionais de *sandboxes* regulatórios (SRs) também refletem a necessidade de salvaguardas relacionadas à proteção ao consumidor, segurança e governança de dados. A exemplo, uma análise realizada pelo Fundo Monetário Internacional - FMI observou que oito SRs aplicadas às Fintechs na Austrália, Canadá, Hong Kong, Malásia, Cingapura, Suíça, Emirados Árabes e Reino Unido possuíam salvaguardas tais como (i) limite no número de consumidores ou valor do serviço oferecido; (ii) obrigações relacionadas ao monitoramento das atividades de testagem e emissão de relatórios; e (iii) salvaguardas específicas de proteção ao consumidor. (IMF (2017), Fintech and Financial Services: Initial Considerations, IMF Staff Discussion Note: SDN/17/05, Disponível em: https://www.imf.org/en/Publications/Staff-DiscussionNotes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985 Acesso em 18/02/2020

	ou depois do período de experiência em regime de *sandbox*[43]. Ressalta-se, ainda, que a implementação de *sandbox* regulatórios contribui para estreitar a relação entre reguladores e empresas inovadoras, de forma que o conhecimento gerado a partir de inovações pode contribuir para criação de novas regulações e políticas públicas. Além disso, também podem ser utilizados, conforme previsto na GDPR, mecanismos de aproximação entre associações e organizações e a autoridade de dados de modo a aproximar seu contato, troca de informações e desenvolvimento institucional. Podem ser previstos selos e certificações de obtenção facilitada e não tão onerosas destinados a agentes de pequeno porte que demonstrem inovação perante a proteção de dados pessoais, bem como esses mesmos mecanismos e código de condutas formulados por associações ou organizações para promover não somente inovação tecnológica, mas também jurídica e institucional. Tais códigos de conduta podem ajudar a diminuir custos com relação à adaptação de regras e permitir o direcionamento de esforços e recursos em outro sentido.

[43] United Kingdom Financial Conduct Authority (2017), Regulatory Sandboxes: Lessons Learned. Disponível em: https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learnedreport.pdf Acesso em 17/02/2021.

Tomada de Subsídios 1/2021

José Renato [redacted]

seg 01/03/2021 22:08

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

[redacted]

1 anexo

Contribuição à ANPD. Sandboxes Regulatórios. V2.pdf;

Prezados,

Segue anexa contribuição para a Consulta Pública referente à aplicação da LGPD para PMEs. A contribuição, voltada à adoção de **sandboxes regulatórios** para proteção de dados, é fruto de um trabalho conjunto entre o Laboratório de Políticas Públicas e Internet - LAPIN e o Abdala Advogados.

Qualquer dúvida, por favor, faça-me saber.

Atenciosamente,

José Renato, Sérgio Alves Jr., Henrique Bawden

--

José Renato Laranjeira de Pereira

Diretor

[redacted]

lapin.org.br

2021 | MARÇO

CONTRIBUIÇÃO À ANPD

SANDBOXES REGULATÓRIOS

ELEMENTOS TEÓRICOS E PRÁTICOS PARA A OPERACIONALIZAÇÃO DE **SANDBOXES REGULATÓRIOS** PARA A PROTEÇÃO DE DADOS PELA ANPD

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

ABDALA ADVOGADOS

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN e Abdala Advogados

Autoria:

Henrique Bawden Silverio de Castro (LAPIN)

José Renato Laranjeira de Pereira (LAPIN)

Sérgio Alves Júnior (Abdala Advogados)

Imagem de Capa:

phive2015, Getty Images Pro

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

ABDALAADVOGADOS

abdalaadvogados.adv.br
/abdalaadvogados

Sobre esta nota técnica

Em 29 de janeiro de 2021, foi aberta uma consulta pública pela Autoridade Nacional de Proteção de Dados - ANPD, para coletar "subsídios sobre a regulamentação da aplicação da Lei nº 13.709/2018 (LGPD) para microempresas e empresas de pequeno porte."

Considerando a relevância do tema para a construção de um ecossistema de inovação e a necessidade de promoção da cultura de proteção de dados pessoais, o **Laboratório de Políticas Públicas e Internet - LAPIN** e o **Abdala Advogados** elaboraram a presente Nota Técnica para abordar elementos teóricos e práticos para a operacionalização de **sandboxes regulatórios** para a proteção de dados pela ANPD.

O documento apresenta exemplos internacionais de uso de sandboxes e aborda os benefícios que podem trazer para o desenvolvimento de novas soluções que garantam maior proteção de dados pessoais. No entanto, apresentamos também os desafios a serem enfrentados para aplicação dessa abordagem regulatória.

Quem somos nós

O **Laboratório de Políticas Públicas e Internet (LAPIN)** é um *think tank* de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

O **Abdala Advogados** é um escritório de advocacia com atuação em temas emergentes de novas tecnologias, proteção de dados pessoais e mercados regulados.

Sumário

I - Introdução 5

II - Regulação responsiva e novas ferramentas regulatórias 6

III - O que são sandboxes regulatórios? 8

IV - Sandboxes regulatórios e proteção de dados 12

V - Um sandbox da ANPD? 15

VI - O caso específico das PMEs e Startups 17

VII - Conclusão 19

I - Introdução

Sandboxes regulatórios têm sido vistos como mecanismos úteis para que reguladores acompanhem o desenvolvimento de novas tecnologias. Sua estrutura lhes garante ferramentas para endereçarem, de forma ágil, os desafios impostos por soluções disruptivas sem que impeçam o desenvolvimento de novos produtos e serviços.

Sandboxes fazem parte de um espectro de modelos regulatórios que pretendem superar a predominância de estratégias de regulação focadas predominantemente na imposição de sanções para lidar com a violação de normas.

Esse tipo de abordagem, comumente chamada de regulação de comando e controle, não tem se mostrado capaz de lidar com o dinamismo existente em diversos setores da economia, em especial o de tecnologia. A mudança de perspectiva da regulação para um modelo colaborativo foi trabalhada por uma série de autores, em especial Braithwaite e Ayres, ao criarem a teoria da regulação responsiva.

Essa visão tem se mostrado mais adequada para lidar com os desafios que aparecem a cada dia para os reguladores: ao trabalhar conjuntamente com o setor regulado, é possível se acompanhar de perto o que está sendo desenvolvido em âmbito normativo e mercadológico e que se compreenda melhor as expectativas do ente regulado sobre a atuação do regulador e vice-versa.

Deste modo, a regulação avança de forma mais ágil e permite que se criem regras mais claras e adequadas para todos os envolvidos, aumentando o grau de *compliance* dos entes do mercado com a legislação vigente ou emergente.

Os sandboxes regulatórios se mostram uma ferramenta efetiva para permitir esse tipo de troca de informações entre reguladores e regulados. Trata-se da criação de um ambiente controlado pelo regulador, onde as empresas podem agir dentro de regras excepcionais cujo objetivo é possibilitar um espaço monitorado no qual autoridades competentes e desenvolvedores de novas soluções possam acompanhar melhor as oportunidades e riscos apresentados pelas inovações e seu tratamento regulatório.

Sandboxes regulatórios têm sido vistos como mecanismos adequados para que reguladores acompanhem o desenvolvimento de novas tecnologias. Sua estrutura lhes garante ferramentas para endereçarem, de forma ágil, os desafios impostos por soluções disruptivas sem que impeçam o desenvolvimento de novos produtos e serviços.

Esta nota técnica irá discutir a possibilidade de adoção de sandboxes regulatórios no âmbito da proteção de dados pessoais pela Autoridade Nacional da Proteção de Dados Pessoais - ANPD, com foco em pequenas e médias empresas e também startups ou empresas de inovação.

A escolha de enfoque em tais formatos empresariais surge pelo fato de poderem ser sujeitos a normas, orientações e procedimentos simplificados e diferenciados no que se refere à proteção de dados pessoais, conforme previsto no art. 55-J, XVIII, da Lei Geral de Proteção de Dados Pessoais - LGPD.

A aplicação de sandboxes regulatórios nesses contextos pode garantir que se tenha grandes ganhos para o setor regulado e para a ANPD, já que abre espaço para o impulsionamentode um ecossistema de inovação que respeite e promova os direitos de autodeterminação informacional e de privacidade da sociedade como um todo.

II - Regulação responsiva e novas ferramentas regulatórias

O uso de ferramentas regulatórias como sandboxes depende não só da disponibilização de recursos humanos e financeiros e de uma abertura da lei para o uso dessa ferramenta, mas também da adoção de uma mentalidade regulatória diferente, que vá além do modelo clássico de comando e controle.

A regulação responsiva consiste em um jogo de persuasão, diálogo (e eventualmente punição) entre esses dois agentes[1]. Nessa dinâmica, há um processo de convencimento mútuo de que as regras e as condições vigentes são adequadas para as duas partes, diminuindo o custo com litigância de ambos os lados[2] ao mesmo tempo que se cria uma cultura organizacional nas empresas de maior cumprimento da lei.[3]

Deste modo, ao fomentar diálogos que pressupõem maior confiança e apoio mútuo entre diferentes atores, a regulação avança de forma mais ágil e permite que se criem regras mais claras e adequadas para todos os envolvidos, aumentando o grau de *compliance* dos entes do mercado com a legislação vigente[4].

A partir desta visão, emprega-se uma série de ferramentas regulatórias que permitem ao regulador atuar de forma mais flexível, podendo modificar a sua atuação conforme os comportamentos dos entes regulados. Um exemplo é a pirâmide regulatória, que permite que o regulador crie uma série de incentivos e punições escaláveis conforme a severidade e ocorrências repetidas de violações de normas pelo regulador.

O sandbox regulatório aparece aqui como um novo desdobramento desta mudança de paradigma regulatório[5]: é a relação de confiança e de cooperação entre regulado e regulador que permite a existência o funcionamento de uma ferramenta como o sandbox, para que haja ganhos para todos os envolvidos, para além da visão superficial de que a regulação apenas serviria como entrave ao desenvolvimento do mercado.[6]

[1] BRAITHWAITE, J., AYRES, I. **Responsive regulation: transcending the deregulation debate**. Nova Iorque, Oxford, 1992. p. 26.
[2] IBIDEM, pg. 95
[3] IBIDEM, pg. 113
[4] IBIDEM, pg. 26
[5] Chiu, I. H-Y, **A Rational Regulatory Strategy for Governing Financial Innovation.** European Journal of Risk Regulation , Volume 8 , Special Issue 4: Special Issue on the EU Public-Health-Security Nexus , December 2017 , pp. 747.
[6] IBIDEM, pp. 743.

III - O que são sandboxes regulatórios?

Os sandboxes regulatórios são um formato de regulação que pretende facilitar o desenvolvimento de produtos e serviços inovadores que podem potencialmente desafiar normas regulatórias já vigentes.

Enquanto é possível traçar padrões em comum entre as versões de sandbox já experimentadas em diferentes setores e países, a sua definição precisa varia bastante entre jurisdições[7]. Para fins desta Nota Técnica, consideramos sandbox regulatório um ambiente normativo formalizado onde participantes de um mercado podem testar novos modelos de negócio, produtos e serviços sujeitos a uma regulamentação especial por um tempo limitado[8].

Nesse sentido, o sandbox permite que o regulador crie um espaço em que nem todas as normas se aplicarão a um ente regulado específico durante a fase de testes de desenvolvimento de uma solução. Nesse espaço, o agente regulado pode atuar sujeito a normas regulatórias mais flexíveis, mas sempre dentro do campo de visão do regulador, de modo a evitar situações onde o regulador seria obrigado a punir o ente regulado por desenvolver um novo produto que viole as normas vigentes.

Isso é feito utilizando-se de uma fase de testes na qual se avalia a adequação desses produtos e serviços à regulação vigente, de modo a identificar se a regulação deve ser modificada para abarcar a inovação ou se esta deve ser adaptada para cumprir o arcabouço normativo vigente. Nesse processo, regulador e regulado mantêm um processo de diálogo constante, de modo a garantir trocas fluidas de informação a respeito do desenvolvimento da solução.

---

[7] UNITED NATIONS SECRETARY-GENERAL'S SPECIAL ADVOCATE FOR INCLUSIVE FINANCE FOR DEVELOPMENT, **EARLY LESSONS ON REGULATORY INNOVATIONS TO ENABLE INCLUSIVE FINTECH: INNOVATION OFFICES, REGULATORY SANDBOXES, AND REGTECH.** Nova Iorque - Cambridge, 2019, pg. 26. Disponível em https://www.unsgsa.org/publications/early-lessons-regulatory-innovations-enable-inclusive-fintech-innovation-offices-regulatory-sandboxes-and-regtech. Acesso em: 12 de fevereiro de 2020.

[8] KNIGHT, Brian R., MITCHELL, Trace E. **The Sandbox Paradox: Balancing the need to facilitate innovation with the risk of regulatory privilege**. Arlington, 2020, p. 7. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590711. Acesso em: 12 de fevereiro de 2020.

Esse formato tem o intuito de permitir, ao fim do período do sandbox, que os agentes envolvidos identifiquem se o produto é ou não adequado à regulação já existe; se é necessário adequar regulações para que o produto seja comercializado; ou se não há possibilidade de desenvolvê-lo sem que se violem direitos previstos no ordenamento jurídico[9].

O sandbox regulatório permite a criação de um contexto de confiança entre regulador e regulado e permite um agir preventivo em vez de um agir reativo ao desenvolvimento de novas tecnologias[10] .

Esses entes poderão atuar com base em regras diferenciadas, desenvolvendo novas tecnologias, normalmente dando maior flexibilidade e diminuindo encargos regulatórios, tendo como contrapartida a necessidade de coletar e compartilhar dados com o regulador sobre as suas atividades, que então tomará decisões sobre a viabilidade de entrada e manutenção dessas tecnologias no mercado.

Vale dizer que a adoção de um método de regulação tal como o sandbox regulatório, além da elaboração de uma estrutura de trabalho colaborativo, também depende de uma mudança de mentalidade do regulador. Este deve adotar uma perspectiva voltada a metas de resultados e performance, com uma abordagem baseada em risco que se adapte às necessidades do regulado para o desenvolvimento de sua solução, de modo a construir seu produto com frequentes direcionamentos do regulador.[11]

A aplicação desse modelo regulatório inicialmente se reservou a fintechs e outras empresas e soluções no mercado financeiro. A britânica Financial Conduct Authority foi a primeira agência reguladora a aplicá-lo, ainda em 2015. De lá para cá, muitas outras seguiram o exemplo inglês, incluindo o Brasil, como no Laboratório de Inovações Financeiras e Tecnológicas - LIFT, concebido pelo Banco Central do Brasil (BCB), e o sandbox regulatório instituído pela Instrução Normativa nº 626 pela Comissão de Valores Mobiliários (CVM).

---

[9] Chen, Christopher C., **Regulatory Sandboxes in the UK and Singapore: A Preliminary Survey** Regulating FinTech in Asia: Global Context, Local Perspectives. Setembro, 2019, pg. 4. Disponível em: https://ssrn.com/abstract=3448901 ou http://dx.doi.org/10.2139/ssrn.3448901

[10] IBIDEM, pg. 8.

[11] DELOITTE CENTER FOR GOVERNMENT INSIGHTS. **The Future of Regulation**. 2018, p. 12. Disponível em: https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html

A adoção de sandboxes se expandiu posteriormente para outros setores econômicos. Isso inclui o setor de *healthtech*, como o Licensing Experimentation and Adaptation Programme (LEAP)[12] do Ministério da Saúde de Singapura, e o sandbox da Care Quality Commission[13], da Inglaterra. Já no setor de aviação, foi recentemente adotado o sandbox do Federal Aviation Administration[14], dos Estados Unidos.

Existem quatro grandes objetivos[15] para criar um sandbox regulatório, e, a partir deles, é possível alterar a sua configuração e a relação entre agentes de mercado e reguladores dentro do sandbox:

- **Inovação**: um dos motivos mais citados na elaboração de sandboxes regulatórias é o fomento à inovação e ao desenvolvimento de novas tecnologias, já que aumenta o nível de segurança jurídica que os participantes do mercado enfrentam ao desenvolver novos produtos;

- **Gerar Benefícios ao consumidor**: sandboxes regulatórios tendem a gerar benefícios a consumidores na medida em que podem gerar maior competitividade no mercado, por meio do acesso a melhores serviços, menores preços, além de ter informações sobre os impactos aos consumidores antes do produto ou serviço ser oferecido ao mercado como um todo[16];

- **Acesso a conhecimento e maior transparência do mercado**: ao desenvolverem os produtos em um ambiente sob supervisão, o regulador tem acesso a informações do mercado em primeira mão e de alta complexidade, já que possibilita um estudo aprofundado sobre as tecnologias desenvolvidas e qual o seu impacto. Além disso, permite um agir não mais reativo, mas sim proativo, por parte do regulador, que, em constante diálogo com o regulado, tem a

---

[12] Ver https://www.moh.gov.sg/content/moh_web/home/our_healthcare_system/RegulatorySandbox.html

[13] Ver https://www.cqc.org.uk/what-we-do/how-we-work-people/regulatory-sandbox.

[14] Ver https://www.faa.gov/uas/programs_partnerships/integration_pilot_program/.

[15] KNIGHT, Brian R., MITCHELL, Trace E. **The Sandbox Paradox: Balancing the need to facilitate innovation with the risk of regulatory privilege**. Arlington, 2020, p. 9. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590711. Acesso em: 12 de fevereiro de 2020.

[16] Para um debate sobre potenciais efeitos negativos de *sandboxes* regulatórios para consumidores, cabe analisar o posicionamento de Americans For Financial Reform (http://ourfinancialsecurity.org/2019/02/joint-letter-80-groups-oppose-cfpbs-no-action-letter-sandbox-proposal/) e o artigo de Jemima Kelly no Financial Times (https://www.ft.com/content/3d551ae2-9691-3dd8-901f-c22c22667e3b).

capacidade de regulamentar situações antes mesmo delas terem impactos sobre consumidores e, especificamente no âmbito de atuação regulatória da ANPD, sobre titulares de dados;

- **Desenvolvimento de mercados**: a adoção de sandboxes regulatórios permite maior desenvolvimento de mercados, já que proporciona um maior avanço nas tecnologias disponíveis em um curto espaço de tempo pelo fato de garantir que sejam desenvolvidas com menor receio, por parte do regulado, de estar infringindo normas.

Esses benefícios se refletem em um sinal verde para o mercado investir em inovação com menos riscos regulatórios atraindo investimentos, a criação de um caminho menos tortuoso para o desenvolvimento de novas tecnologias, com menores custos e maior velocidade[17]. Também permite maior direcionamento da atuação do regulador para pautas consideradas importantes para os reguladores e um aumento da confiança entre mercados e organismos estatais, a partir do estreitamento de relações que ocorre a partir da realização do sandbox regulatório.

Por outro lado, apesar dos benefícios identificados na adoção de *sandboxes,* o modelo impõe alguns desafios para sua implementação. Espera-se do regulador que tenha recursos humanos e tecnológicos suficientes para gerir o sandbox e conseguir analisar os dados que serão coletados. Além disso, uma abertura em primeiro momento que descambe em ações retaliatórias por parte do regulador pode acabar prejudicando a criação de uma relação de confiança entre ambas as partes[18].

Também há dificuldades relacionadas à própria natureza do mercado e dos produtos envolvidos: a depender do grau de complexidade e do impacto que poderá advir da solução a ser oferecida, a criação de um sandbox regulatório não terá muitas vantagens pela impossibilidade de flexibilizar regulações devido aos riscos envolvidos nas atividades. Isso poderia ocorrer em parte, por exemplo, no setor de saúde, ou pela própria natureza do mercado, como no setor elétrico.

---

[17] WECHSLER, M., PERLMAN, L., GURUNG, N. The State of Regulatory Sandboxes in Developing Countries. Nova Iorque, 2018, p. 24. Disponível em: https://ssrn.com/abstract=3285938.

[18] WECHSLER, M., PERLMAN, L., GURUNG, N. **The State of Regulatory Sandboxes in Developing Countries**. Nova Iorque, 2018, p. 26. Disponível em: https://ssrn.com/abstract=3285938.

Além disso, um risco específico de sandboxes em países em desenvolvimento é que pode ocorrer falta de transparência com a sociedade como um todo na realização do sandbox, aumentando o risco de captura do regulador diante do estreitamento de relações e de criação de privilégios[19]. Essa transparência se mostra necessária, sendo possível inclusive a inclusão de grupos da sociedade civil para realização de supervisão, tendo em vista que a sua participação dentro de fenômenos regulatórios diminui o risco de captura do regulador[20], garantindo o bom funcionamento do sandbox regulatório.

IV - Sandboxes regulatórios e proteção de dados

Como mencionado anteriormente, a implementação de sandboxes regulatórios não está restrita à área de finanças, sendo aplicada para vários setores da indústria. A partir dessa abertura, é possível se indagar sobre a viabilidade da criação de um sandbox regulatório no campo da proteção de dados pessoais.

A adequação de *sandboxes* regulatórios para a proteção de dados se dá também porque o tratamento de dados pessoais é condição necessária para que haja a viabilização de inúmeros modelos de negócios em indústrias como a de *healthtechs* e de *fintechs*, por exemplo.

Reflexo disso é o fato de que já foram criados sandboxes regulatórios com foco em proteção de dados pessoais em outras jurisdições. Nesse sentido, podemos citar os *sandboxes* do Information Commissioner's Office (ICO), da Inglaterra, da Associação dos Países do Sudeste Asiático (ASEAN), o sandbox do Infocomm Media Development Authority - IMDA, de Singapura[21] e o sandbox regulatório da Superintendencia de

[19] IBIDEM, p. 27.
[20] BRAITHWAITE, J., AYRES, I. Responsive regulation: transcending the deregulation debate. Nova Iorque, Oxford, 1992, pg. 71.
[21] BUSINESS AT OECD. **Regulatory Sandboxes for Privacy: Analytical Report**. 2020, pg. 3. Disponível em: https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

Industria y Comercio, da Colômbia[22]. Também é possível verificar que a Comissão Europeia, ao tratar de Inteligência Artificial, já vislumbrou a utilização de sandbox regulatórios[23].

Um dos principais atrativos em relação aos *sandboxes* regulatórios de proteção de dados é a capacidade de melhorar a regulação com base em princípios que os reguladores têm adotado em frente às incertezas criadas com a introdução e desenvolvimento de novas tecnologias, novos usos de dados e rápida inovação[24]. Nesse modelo de sandbox, o foco é o teste de produtos e serviços antes que entrem no mercado, tornando visíveis riscos envolvidos nos tratamentos e garantindo que se sigam uma abordagem de *privacy by design* e *default* desde o início de sua criação.

Exemplo disso ocorreu com o IMDA, que, em conjunto com o Facebook, criou um sandbox onde várias startups, com a colaboração de especialistas da indústria e com a supervisão dos reguladores, desenvolveram maneiras de concretizar notificação e consentimento dinâmico e sua implementação em uma série de serviços, criando inovação e aumentando o grau de proteção aos dados pessoais dos indivíduos.[25]

Outro exemplo é o sandbox do ICO, que possui como um dos seus focos o design de padrões de proteção de dados pessoais voltados para menores de idade[26]. O sandbox do regulador britânico já tem publicados seus primeiros relatórios, englobando

---

[22] Ver https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F26973

[23] EUROPEAN COMISSION. **ANNEX TO THE COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence**. Brussels, 2018, pg. 8

[24] BUSINESS AT OECD. **Regulatory Sandboxes for Privacy: Analytical Report**. 2020, pg. 13. Disponível em: https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

[25] BUSINESS AT OECD. **Regulatory Sandboxes for Privacy: Analytical Report**. 2020, pg. 15. Disponível em:https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

[26] Ver https://ico.org.uk/media/for-organisations/documents/2618112/our-key-areas-of-focus-for-regulatory-sandbox.pdf

tecnologias na área da saúde[27], de reconhecimento biométrico[28], compliance[29], e até mesmo experiência do usuário em aeroportos[30], permitindo a identificação de riscos que possam existir e facilitando a construção de inovações que já entrarão no mercado adequadas ao nível de proteção de dados pessoais exigido pelo ICO.

Existem também desafios peculiares à instalação de sandboxes no campo da proteção de dados.

A aplicação de regulamentações de outras indústrias, em especial naquelas áreas que se mostram fortemente reguladas, como saúde e setor bancário, pode gerar entraves caso não sejam feitos em conjunto com os reguladores específicos desses setores por meio de acordos de cooperação.

Também existem questões envolvendo a dificuldade de atuação com outros reguladores em casos de companhias transnacionais, em especial em casos onde não haja compatibilidade entre as legislações de proteção de dados pessoais dos diferentes países e ocorram transferências internacionais de dados.

Por fim, a falta de recursos dos reguladores é outra questão a ser considerada, ainda mais em casos em que o regulador ainda precisa ser devidamente estruturado, como é o caso da ANPD.[31]

---

[27] Report e resultados disponíveis em: https://ico.org.uk/media/for-organisations/documents/2618905/nhs-digital-regulatory-sandbox-final-report.pdf

[28] Report e resultados disponíveis em: https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf

[29] Report e resultados disponíveis em: https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf

[30] Report e resultados disponíveis em: https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf

[31] BUSINESS AT OECD. **Regulatory Sandboxes for Privacy: Analytical Report**. 2020, pg. 19. Disponível em:https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

V - Um sandbox da ANPD?

Mesmo que a adoção de um sandbox regulatório seja desejável para a ANPD de modo a trazer melhorias para o ecossistema regulatório, é necessário que se faça indagações em torno de dois pontos:

1. existe abertura legislativa para a criação de um sandbox regulatório?
2. quais os recursos humanos e tecnológicos necessários para o seu bom funcionamento?

Não há dispositivos de lei em sentido formal no ordenamento jurídico brasileiro que disponham expressamente que os órgãos e agências reguladoras possuem o poder de criar sandboxes regulatórios.

Contudo, o BACEN, a SUSEP e a CVM criaram os seus sandboxes regulatórios mesmo sem essa autorização expressa da lei, utilizando-se de normativos infralegais para legitimar a existência e a delinear o funcionamento dos sandboxes. Tal solução não foi questionada no âmbito judicial e se manteve estável até hoje, o que demonstra a aceitação dessa atuação tanto pelo Estado quanto pelo mercado e pela sociedade civil.

O uso deste instrumento legal para a instituição do sandbox deriva da sua natureza legal: em última instância, a participação no sandbox regulatório pode ser caracterizada como uma autorização a um regime legal diferenciado[32], que é criado pela própria agência reguladora por meio da emissão de normativos infralegais exclusivos a um ente regulado específico.

Como os normativos que possuem a sua aplicabilidade alterada são aqueles de competência da própria agência reguladora, não há problema na emissão de tal autorização diferenciada[33]. O que acontece é uma mera manipulação do arcabouço normativo do próprio ente regulador, que, diante de condições pré-estabelecidas,

[32] Para entender melhor a referida tese, recomenda-se a leitura do Parecer 374/2019-BCB/PGBC do Banco Central do Brasil. Disponível em: https://revistapgbc.bcb.gov.br/index.php/revista/issue/view/32/P4%20V.14%20-%20N.1

[33] CARVALHO, D. T. , MAIA, A. F., OLIVEIRA, W. P R., DOS SANTOS, M. M. e COZER C. Parecer 374/2019-BCB/PGBC. Revista da PGBC – V. 14 – N. 1 – Jun. 2020 .pg. 211. Disponível em: https://revistapgbc.bcb.gov.br/index.php/revista/issue/view/32/P4%20V.14%20-%20N.1

concede uma autorização para que alguns entes do mercado funcionem em regime legal diferenciado.

Situação diferente seria se o sandbox regulatório se propusesse a alterar ou suspender a aplicabilidade de leis em sentido formal. Nesse caso, seria necessária a edição de um dispositivo legal que possibilitasse tal ação.

Logo, não há nenhum tipo de entrave legal para o funcionamento de sandboxes regulatórios no direito brasileiro, sendo possível a sua criação por meio de normativos infralegais por órgãos e agências reguladoras[34].

A segunda questão levantada se refere aos recursos para o bom funcionamento do sandbox regulatório. Uma questão que merece atenção é que, antes de tudo, é necessário capacidade de análise de dados para que o trabalho feito dentro do sandbox não seja feito em vão.

Como já mencionado, é necessário que exista um time dedicado para a coleta e análise dos dados do sandbox, dispondo de recursos humanos e de infraestrutura tecnológica o bastante. No caso específico da ANPD, que possui estrutura ainda em construção e relativamente diminuta frente a outros reguladores, isso pode ser um grande gargalo.

Como meio para resolver isso, uma solução pode ser desenvolver o sandbox regulatório conjuntamente com o setor privado, usando dos recursos disponibilizados por eles, em especial os tecnológicos. O grande exemplo desse tipo de solução foi o sandbox regulatório do IMDA de Singapura, que foi feito em colaboração com o Facebook, havendo uma supervisão do IMDA e o uso de recursos tecnológicos e humanos do Facebook.

Tal solução também foi utilizada no Brasil por meio do chamado LIFT. Em seu escopo, foi firmado acordo de cooperação técnica entre o Banco Central e a Federação Nacional das Associações de Servidores do Banco Central (Fenasbac), para que se utilizasse recursos humanos e financeiros dos participantes privados para promover o funcionamento de um *sandbox* regulatório.[35]

---

[34] IBIDEM, pg. 209.

[35] Ver https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-iniciativa-de-sandbox-do-mundo-04092019 e

Logo, através de parcerias com o setor privado, é possível que se monte um modelo de sandbox regulatório que seja viável mesmo em condições de recursos escassos, sendo necessário apenas que se façam acordos que permitam a utilização de infraestrutura e recursos humanos dos entes participantes do sandbox regulatório.

VI - O caso específico das PMEs e Startups

Por fim, é necessário comentar as especificidades envolvendo um sandbox regulatório para PMEs e startups, assunto-alvo da consulta pública realizada pela ANPD. A questão a ser respondida é a viabilidade de se criar sandboxes regulatórios específicos a empresas com essas características.

Não há na literatura do tema nenhum indicativo de que haveria restrições à participação de pequenas ou médias empresas. Inclusive, as recomendações vão no sentido contrário, de que haver uma gama de empresas de diversos tamanhos seria beneficial para o sandbox.[36] Alguns sandboxes inclusive trazem limites ao tamanho das empresas que abrangerão, como o do Australian Securities and Investments Commission (ASIC)[37].

Um argumento a favor da inclusão de PMEs e startups em sandboxes regulatórios é exatamente o potencial de inovação que esses negócios possuem, ainda mais levando em conta a tendência das startups de tentar introduzir tecnologias disruptivas no mercado. A entrada dessas empresas em um sandbox ajudaria os reguladores a lidar melhor com tais tecnologias, coletando dados desde o início da sua concepção e criando uma maior segurança jurídica para as empresas.

---

https://www.bcb.gov.br/content/acessoinformacao/Documents/acordos/Primeiro-Aditivo-Acordo-Fenasbac.pdf.

[36] BUSINESS AT OECD. **Regulatory Sandboxes for Privacy: Analytical Report**. 2020, pg. 19. Disponível em:https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

[37] BAKER MCKENZIE. International Guide to Regulatory Fintech Sandboxes. 2018, pg. 4 . Disponível em: https://www.bakermckenzie.com/en/-/media/files/insight/publications/2018/12/guide_intlguideregulatorysandboxes_dec2018.pdf

Tal posição parece ter sido corroborada pelo legislador brasileiro. A LGPD traz no art. 55-J, inciso XVIII, que trata das competências da ANPD, a possibilidade do órgão (da administração direta) o poder de "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".

Essa abertura da lei para a criação de normas diferenciadas a startups garante espaço amplo para a criação de *sandboxes* regulatórios sobre proteção de dados.

Além disso, o projeto de lei que institui o Marco Legal de Startups e Empreendedorismo Inovador (MLSEI) dispõe de modo expresso sobre a possibilidade de instituição de sandboxes regulatórios para startups.

Apesar das alterações promovidas pela Câmara dos Deputados e Senado Federal à redação original do Projeto de Lei Complementar (PLP) nº 249/2020, de autoria do Poder Executivo, o texto que retorna à Casa de Origem mantém a mecânica e previsão desse instrumento.

Para o caso específico de startups e proteção de dados pessoais, a redação do projeto de lei amplifica a capacidade institucional de a ANPD instituir seu sandbox, inclusive com outros reguladores, por meio de colaboração.

Caso opte por seguir este caminho e a lei venha a ser sancionada, bastaria à ANPD dispor sobre o funcionamento do programa de ambiente regulatório experimental e estabelecer: (i) os critérios para seleção ou qualificação do regulado, (ii) a duração e o alcance da suspensão da incidência e (iii) as normas abrangidas.[38]

Se a ANPD desejar promover um sandbox de modo conjunto com outro regulador, a Autoridade deverá simplesmente firmar relação de colaboração com o órgão ou entidade da administração pública com competência de regulamentação setorial pertinente.

[38] Na versão aprovada pelo Senado Federal, a matéria está disposta no "Capítulo V - Dos Programas de Ambiente Regulatório Experimental (Sandbox Regulatório)".

Essa previsão de cooperação entre reguladores pode acabar com problema significativo que envolvia as empresas cujos produtos estavam sob a regulação de mais de um ente, como aquelas que atuam no mercado de seguros privados, que encontraram problemas na participação no sandbox regulatório da CVM e da SUSEP ao mesmo tempo.

Se aprovada a redação do MLSEI sobre sandboxes regulatórios, Executivo e Legislativo brasileiros terão a oportunidade de inaugurar o ambiente jurídico favorável para solucionar entraves de convergência tecnológica e fronteiras setoriais regulatórias já identificados em sandboxes de outras jurisdições como Colômbia e Alemanha. Por consequência, haverá ganhos para a ANPD, seus regulados e titulares de dados pessoais.[39]

Considerando o desenvolvimento acelerado de novas tecnologias que fazem uso de dados pessoais nos mais diversos setores da economia, certamente há lugar para regulá-los a partir de sandboxes. O uso de tecnologias que fazem uso massivo de dados pessoais e que perpassam diferentes setores regulados exigem formas disruptivas de regulação. O sandbox seria um local apropriado para testar esse tipo de solução, pelo fato de limitar sua experimentação em tempo e espaço e ao mesmo tempo garantir a supervisão integral do regulador.

VII - Conclusão

O uso de sandboxes regulatórios no âmbito da proteção de dados não é apenas possível, mas uma **solução** que ataca questões centrais da regulação digital, tal como a dinamicidade das inovações tecnológicas, a existência de negócios que são regulados

[39] Ver ALVES, Sérgio Garcia; LARANJEIRA, José Renato de. Marco Legal das Startups, LGPD e sandboxes regulatórios em colaboração. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/marco-legal-das-startups-lgpd-e-sandboxes-regulatorios-em-colaboracao-21122020. Acesso em: 1º de março de 2021.

por múltiplos entes, a necessidade de fomento à área e a construção de um ambiente regulatório bom para todos os envolvidos.

Contudo, devem ser levados em conta **requisitos estruturais para a sua utilização**, como a disponibilidade de recursos humanos e tecnológicos e uma boa relação entre o mercado e a ANPD. Além disso, não se deve subestimar a necessidade de construir um regime legal de funcionamento do sandbox regulatório claro, transparente e que abarque as necessidades de todos os participantes.

É necessário um **planejamento de longo prazo** pela ANPD para a adoção de tal ferramenta, diante dos custos e da sua dinâmica de funcionamento. Superadas essas barreiras, o sandbox regulatório será uma ferramenta que pode trazer muitos ganhos para a ANPD, para o mercado e para a proteção de dados pessoais no Brasil.

Tomada de Subsídios 1/2021 | Instituto Nacional de Proteção de Dados

Rafael Reis [redacted]

seg 01/03/2021 22:33

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

1 anexo

Modelo_envio_de_contribuicoes PMEs.pdf;

SENHOR DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD

O **INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS**, pessoa jurídica de direito privado, sem fins lucrativos, inscrita no CNPJ/MF sob o nº 37.415.768/0001-36 com sede à Rua Jacarezinho, nº 1459, bairro Mercês, Curitiba, Paraná, CEP 80.810-130, neste ato representada por seu secretário-executivo, Rafael Almeida Oliveira Reis, vem respeitosamente à presença de Vossa Senhoria apresentar as contribuições criadas pelo comitê instituído para debater e sugerir políticas de proteção de dados voltadas para pequenas e médias empresas e startups, visando o aprimoramento do sistema normativo-regulatório no contexto do objeto da consulta proposta pela ANPD, conforme tomada de subsídios de nº 1/2021.

Se envolveram nos trabalhos os seguintes diretores, membros e fellows do INPD:

Cláudio Lucena – Diretor Técnico e de Parcerias Estratégicas Internacionais
Rafael Mosele – Diretor das Relações do Trabalho
Gisele Gadelha – Diretora de Parcerias Estratégicas com Setor Privado
Elizabeth Pelisson – Fellow
Martha Leal – Fellow
Carolina Margonari - Fellow
Victor Prata – Membro Associado

O documento modelo com as contribuições encontra-se anexo a este e-mail.

Att.

Diretoria Executiva INPD
diretoria@inpd.com.br
Instituto Nacional de Proteção de Dados – INPD
CNPJ: 37.415.768/0001-36

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS - INPD

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	**O INPD - Instituto Nacional de Proteção de Dados é uma Associação civil sem fins lucrativos e que visa fomentar a pesquisa, o debate e auxiliar nas políticas voltadas à proteção de dados.** **Com o objetivo de contribuir no desenvolvimento dos temas que são objeto da presente chamada de subsídios, o INPD, reconhece e celebra a importância da iniciativa desta Autoridade Reguladora no chamamento da sociedade para participação na formação de normas e parâmetros que, sem dúvida alguma, impactam a inovação, o desenvolvimento econômico e a proteção de dados pessoais.** **Os seguintes tópicos são abordados neste documento, para análise desta Autoridade Reguladora, como contribuição no desempenho das tarefas que incumbem a proteção de dados em consonância com o desenvolvimento econômico, tecnológico e a inovação, fundamentos assegurados pelo art. 2, da Lei n. 13.709/18, particularmente no escopo da contribuição que foi solicitada:**

	1) **Flexibilização de nomeação de encarregado;** 2) **Flexibilização da obrigatoriedade dos registros das atividades;** 3) **Flexibilização na prática de anonimização de dados;** 4) **Promoção de planos de privacidade inclusivos;** 5) **Reequilíbrio da responsabilidade civil perante o titular de dados;** 6) **Criação de fóruns para realizar constante atualizações regulatórias adaptadas às particularidades das startups.** 7) **Adoção do critério de dupla visita, a exemplo do art. 627 da CLT;**
Existem sugestões para endereçamento do problema?	**1)Flexibilização da nomeação de encarregado, conforme art 41: O INPD - Instituto Nacional de Proteção de Dados sugere a dispensa da obrigatoriedade da indicação da figura do encarregado e em consequência, a supressão da hipótese de multa pelo regulador nacional, para empresas de pequeno porte.** **2)Dispensa dos registros das atividades de tratamento, avaliação de impacto e avaliação de impacto para LIA, conforme art. 37: O INPD sugere a dispensa da obrigatoriedade na confecção e manutenção dos registros das operações e avaliação de impacto e a supressão da multa pelo regulador para empresas de pequeno porte. Em caso de suspeita de tratamento de dados pessoais com potencial de risco aos direitos dos titulares, propõe-se que o regulador solicite o Relatório de Impacto, com prazo superior em dobro, ao concedido aos demais agentes que não se enquadrem na categoria de PMEs. Em paralelo, incentiva-se o fornecimento de manuais explicativos relacionados às atividades de registros, com passo a passo, para melhor execução das tarefas, em linguagem de fácil compreensão, o que sem dúvida, auxiliará as mesmas no processo de adequação a LGPD.**

	3)Flexibilização da anonimização de dados: O INPD propõe a flexibilização do dever por parte das empresas de pequeno porte, em anonimizar, sempre que possível, os dados pessoais, quando requeridos pelo titular de dados pessoais e a supressão da multa correspondente pela ANPD. Apesar da proposta de mitigação de uma obrigação, justificada pelo contexto setorial, o INPD incentiva a conscientização da importância da técnica que objetiva auxiliar as empresas a proteger os dados pessoais que possuem, podendo de acordo com a técnica utilizada e o resultado obtido, desonerar ou minimizar a responsabilidade dos agentes de tratamento por danos causados aos titulares. **4) Programa de privacidade (Art. 50 LGPD): No que se refere aos programas de privacidade previstos no Art. 50 LGPD, cabe salientar que as regras de boas práticas e de governança deverão ser publicadas, bem como poderão ser reconhecidas e divulgadas pela autoridade nacional (parágrafo terceiro). Em prática, códigos voluntários de conduta poderão emergir setorialmente, tendo a capacidade de estandardizar os procedimentos de todo um ramo comercial uma vez que serão legitimados pela ANPD. Tal processo de estandardização poderá ser utilizado ainda para classificar companhias como confiáveis ou não no que toca à adequação à LGPD, resultando consequentemente na exclusão daquelas consideradas incapazes de provar de antemão por meio da adesão às regras de boas práticas e de governança sua conformidade com a legislação nacional de proteção de dados. Portanto, é importante que, ao se definir tais regras, PMEs tenham espaço suficiente para vocalizar seus interesses, prioridades e potenciais desafios. Em suma, as regras de boas práticas e de governança deverão ser estabelecidas com forte envolvimento das PMEs. Cabe ressaltar que não raras vezes as regras de boas práticas e de governança tendem a ser criadas por grandes empresas, refletindo assim sua realidade, e em muitas ocasiões causando uma concentração de mercado. Sugere-se, então, garantir que as regras de boas práticas e de governança sejam traçadas de forma transparente, democraticamente e sem impor um ônus excessivo às PMEs.** **5) Responsabilidade civil do controlador PME na cadeia de tratamento: No tocante à responsabilidade civil do controlador PME na cadeia de tratamento de dados, foram**

	identificados dois desafios cruciais, resultando assim em um maior problema regulatório. **O primeiro desafio seria a assimetria informacional entre PMEs atuando como controladores e delegando tanto tratamento como armazenamento de dados pessoais a operadores que são grandes companhias e/ou que estão localizadas no exterior, ou ainda que recorrem a data centers fora do Brasil (seja como ponto principal de processamento, seja como back up).** **Vale ressaltar que transferência internacional de dados fora das condições previstas no Art. 33 pode ser considerada em si uma violação à LGPD e pode-se entender que haverá um dano social, posto que a transferência (ainda que para mero fim de back up) será feita para um país de forma não segura (incluindo a possibilidade de vigilância indevida dos titulares de dados).** **O segundo seria a assimetria negocial entre PMEs enquanto controladores e operadores que são *big players*, impondo unilateralmente termos de serviço sem ter em conta as especificidades da legislação brasileira. Identificou-se como problema regulatório decorrente que o Art. 42, §1, II LGPD impõe responsabilidade objetiva às PMEs envolvidas em danos aos titulares de dados sem, entretanto, prever uma repartição justa conforme culpa, conhecimento prévio e impacto nas finanças da empresa. Como consequência, PMEs no papel de controladores podem estar sujeitas à falência devido a fatores que são excessivamente onerosos (e, portanto, não factíveis) para serem monitorados por organizações com sérias restrições orçamentárias e ausência de know-how em sua equipe. De forma indireta, responsabilizar PMEs em primeira linha sem avaliar conjuntamente o papel do operador poderá resultar em uma concentração do mercado, onde somente grandes empresas terão capacidade de gerir os riscos envolvidos e suportar suas possíveis consequências. Sugere-se, então, uma mitigação da responsabilidade imediata das PMEs com a possibilidade de invocar conjuntamente a responsabilidade dos operadores nos autos processuais.** **6) Sandbox para startups em proteção de dados: No relacionado às startups, verificou-**

	se como desafio o fato que, como pontuado no parágrafo segundo do Art.65-A da LC n. 123/2006, as atividades corporativas das startups envolvem: 1- inovações em condições de incerteza, 2- requerem experimentos e validação constantes, 3- seus produtos ou serviços são oferecidos em contexto de comercialização experimental provisória antes de avançar rumo à comercialização plena futuramente nas fases de tração e scale-up. Consequentemente, os potenciais problemas regulatórios seriam que as startups operam no que se chama contexto de ambiguidade, onde se desconhece em grande parte quais são os riscos envolvidos e o resultado real das atividades, e de alta complexidade. Além disso, no caso das startups envolvidas em inovações de circunvenção - ou seja, aquelas que não se enquadram adequadamente a nenhum regramento específico -, o desafio será aplicar a LGPD de forma rapidamente adaptada e equilibrada. Sugere-se, então, pensar métodos flexíveis, mas sempre buscando garantir transparência, de conformidade entre LGPD e as inovações fomentadas pelas startups. **7) Adoção do critério da dupla visita de forma análoga ao utilizado no Direito do Trabalho: Sugere-se a adoção do critério da dupla visita para PMEs, cuja a finalidade seria a orientação, em duas visitas ao estabelecimento do agente de tratamento, com o objetivo de inspeção do ambiente de trabalho e instrução para saneamento de eventuais irregularidades e a segunda visita, para verificação da adequação das medidas apontadas na visita anterior. Art. 627 e 627- A da CLT. O mesmo critério poderia ser estendido às empresas de pequeno porte, tornando inválida qualquer autuação pelo Órgão Regulador, sem prévia visita ao agente.**
Quais são as oportunidades relacionadas ao tema?	**1) Programa de privacidade (Art. 50 LGPD): Regras de boas práticas e de governança bem definidas e que integrem PMEs em todas as etapas desde a ideação até a implementação podem conferir maior segurança e clareza no cotidiano corporativo, reduzindo assim os altos custos informacionais que PMEs teriam para se adequar e se manter em conformidade com a LGPD.** **2) Responsabilidade civil do controlador PME na cadeia de tratamento: Garantir uma efetiva compensação por danos aos titulares de dados ao passo que promove uma maior observância da LGPD por parte de todos operadores com infraestruturas ou**

	sede corporativas localizadas quer nacional, quer internacionalmente. **3) Sandbox para startups em proteção de dados: Promover inovação ao passo que se resguarda os direitos fundamentais dos titulares de dados numa dinâmica que se pode chamar de *smart regulation,* como explicado por Gunningham e Sinclair, "Designing smart regulation". Contudo, não se deve enfraquecer uma abordagem centrada em direitos e princípios fundamentais às inovações, quer incremental, quer disruptiva.**
Quais são as experiências internacionais sobre o tema?	**1)Da Flexibilização do encarregado: O Regulamento Europeu – RGPD – no. 2016/579, de 27 de abril de 2016, em seu art. 37, (1) *a* a *c*, adota uma lógica inversa à norma brasileira, e apenas dispõe expressamente sobre as hipóteses de designação obrigatória, que são: a) quando o tratamento é realizado por uma autoridade ou organismo público; b) quando as atividades principais dos agentes de tratamento consistem em operações de tratamento que requerem monitoramento regular e sistemático em grande escala; ou, c) quando as atividades principais dos agentes consistem em grande escala de categorias de dados sensíveis ou dados pessoais relativos a condenações criminais.** **Nesse sentido também, as orientações do Grupo de Estudos do Art. 29, WP 243. Essa dinâmica libera sem maior burocracia as demais instituições, entre as quais as que são objeto desta demanda, do encargo, desde que o grau de risco das operações de tratamento de dados não esteja já no patamar estabelecido como de alerta, exigindo a indicação de encarregado.** **2)Da desobrigação dos registros de operações de tratamento: O Regulamento Europeu - n. 2016/579, em seu art. 30 dispõe sobre a obrigatoriedade dos agentes de tratamento em conservar os registros das operações, nos incisos 1 e 21, entretanto, no inciso 5, excetuam-se destas obrigações, àquelas empresas com menos de 250 funcionários, a menos que o tratamento efetuado seja suscetível de implicar em elevados riscos aos titulares.** **3)Da flexibilização da obrigatoriedade da anonimização de dados: O Regulamento Europeu - n. 2016/579, diferentemente da LGPD, não elenca, no rol dos direitos dos titulares - art. 13 à 21- o direito à anonimização.**

	4) Programa de privacidade (Art. 50 LGPD): Existe a iniciativa do EU Cloud Code of Conduct a nível regional. Trata-se de um mecanismo voluntário que procura estabelecer regras de boas práticas e de governança na área da proteção de dados e cibersegurança no setor de serviços de nuvem. Contudo, PMEs não têm direito de voto (ver https://eucoc.cloud/en/participate/pricing/), o que prejudica a legitimidade e a ampla adesão a esses *standards*. **5) Responsabilidade civil do controlador PME na cadeia de tratamento:** Há um debate doutrinário na União Europeia se PMEs deveriam ser equiparadas a consumidores, e assim, beneficiarem-se de normas mais protetivas do que aquelas regendo contratos B2B (cf. Loos e Samoy (2017), "The Position of Small and Medium-Sized Enterprises in European Contract Law"). Além disso, em outras áreas jurídicas, discute-se elevar o grau de proteção para as PMEs, entendendo-se por cláusulas contratuais injustas aquelas que não seriam individualmente negociadas com impactos negativos concretizados, noticiando-se ainda outro elemento: a falta de transparência em tais cláusulas contratuais (ver Art. 86(1) em combinação com Art. 83(2) da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um direito europeu comum da compra e venda). No mais, vale a pena destacar a decisão australiana de 2017 no caso Australian Competition and Consumer Commission v JJ Richards & Sons Pty Ltd em que se estendeu a proteção jurídica garantida sob a legislação nacional de defesa do consumidor às PMEs por se considerar que o contrato standard imposto pela grande companhia continha cláusulas abusivas (cf. http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2017/1224.html). Portanto, reconhecendo-se o nexo direto entre relações comerciais desproporcionais e responsabilidade civil, é possível identificar a necessidade de formas mais protetivas para PMEs também no campo da responsabilização face aos titulares de dados. **6) Sandbox para startups em proteção de dados:** Tem-se proposto como metodologia/caminho para atender as particularidades das *startups regulatory sandboxes.* Como Dan Quan salienta, a grande importância das *regulatory sandboxes* é que: "With innovation taking place at a breakneck speed, regulatory agencies need to actively seek to understand the benefits and risks of innovation, while developing

	appropriate policies, guidance, and/or regulations to reap those benefits, protect consumers" (cf. https://pacscenter.stanford.edu/a-few-thoughts-on-regulatory-sandboxes/).
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	**Os critérios sugeridos para definição de agentes de tratamento de pequeno porte são os seguintes:** **I) Empresas que tenham faturamento bruto anual até o limite máximo estabelecido no art. 3, II, da Lei Complementar n. 123, de 14 de dezembro de 2006;** **II) Empresas que não tenham como objeto social o tratamento de dados pessoais, ou cuja atividade fim não seja dependente do tratamento de dados pessoais.** **Programa de privacidade (Art. 50 LGPD)** **1. Sugere-se que sejam baseados no Art. 3 da Lei Complementar n. 123/2006, criando-se assim uma coerência sistêmica.** **Responsabilidade civil do controlador PME na cadeia de tratamento** **No tocante à responsabilidade civil, uma maior extensão aos operadores deve ocorrer com base em cinco critérios cumulativos:** **1. o controlador é classificado como PME, conforme critérios objetivos inspirados em outras legislações ou diretrizes brasileiras;** **2. o controlador não trata dados sensíveis, nem realiza tratamento de dados em larga escala, o que exigiria mecanismos de controle e monitoramento mais robustos, e consequentemente, uma responsabilidade acrescida;** **3. o operador é uma empresa de grande porte, caracterizando assim uma assimetria na relação entre controlador e operador;** **4. o operador impõe unilateralmente seus termos de serviço às PMEs, caracterizando uma assimetria negocial;** **5. o dano ou a violação em causa decorre da conduta do operador.**

	Sandbox para startups em proteção de dados **1. Artigo 65-A, *caput*, da Lei Complementar n. 123/2006 define como *startup* as iniciativas empresariais de caráter incremental ou disruptivo. Em seu parágrafo primeiro, o artigo referido esclarece que: "Para os fins desta Lei Complementar, considera-se startup a empresa de caráter inovador que visa 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".**
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)?	**Ações realizadas pelas Autoridades do Reino Unido, Itália e Espanha.** **ICO - Reino Unido.** **· Trabalhando fortemente na parte educacional no site da autoridade, disponibilizando *checklist* de conformidade, guias/manuais com dicas a respeito dos pontos principais sobre adequação para esse setor e canal de atendimento via telefone/e-mail.** **https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/whats-new/blogs/15-things-all-small-businesses-need-to-know-about-data-protection/** **https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/** **· Indicando os pontos básicos necessários para adequação.** **· Utilizando verificador de base legal online, para auxiliar essas empresas na identificação sobre qual base legal poderão utilizar.**

	· **Concedendo prazo de 72 horas para reportar incidentes.** · **Trabalhando na conscientização sobre o tema segurança da informação.** **Garante - Itália.** · **Oferecimento de oportunidade para criação de software para apoiar a compreensão e conformidade com a lei para essas empresas.** **https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9464663** **AEPD - Espanha.** · **Realização de pesquisas para entender o cenário de adequação dentro de empresas desse porte.** **https://www.aepd.es/sites/default/files/2019-10/estudio-proteccion-de-datos-aepd-cepyme.pdf** · **Criação de orientação especial para empresas desse porte, com facilidades de localização de documentos e informações para fins de adequação.** **https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/pymes**
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	**Os impactos para agentes de pequeno porte na manutenção de registros das operações, apesar de se traduzirem em boas práticas, podem ser negativos, uma vez que demandam investimentos com recursos humanos e técnicos, que podem vir a onerar de forma desequilibrada essas categorias, prejudicando o ecossistema econômico e a concorrência.**

Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	**Um relevante impacto decorrente da obrigatoriedade de nomeação de um encarregado é o elevado custo com a contratação de profissional especializado para o desempenho da função, podendo pesar e comprometer a operação dos agentes de tratamento destas categorias.**
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	**Os impactos para agentes de tratamento de pequeno porte na elaboração do relatório de impacto estão na complexidade da análise e da documentação, que demandam mão de obra especializada e consequente dispêndio de recursos financeiros na contratação de profissionais. Além disso, adaptar a operação a fatores externos também passa a ser uma ação complexa e mais cara.**
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?	**Modelos de negócios que utilizem dados sensíveis e dados de crianças e adolescentes evidentemente têm menor margem de manobra, seja em função das próprias restrições da LGPD, seja em virtude da compatibilização necessária com fatores e princípios que vão além da legislação específica, como os interesses jurídicos fundamentais por trás dos dados sensíveis, e o melhor interesse, no caso de crianças e adolescentes. São tratamentos que devem naturalmente exigir mais cuidado, modelos de negócio que precisam estar sob supervisão mais rígida dada a delicadeza dos interesses contrapostos, e tudo isso também envolve análise de impacto mais ampla, mais complexa, restrição a determinadas alternativas de iniciativa empresarial, o que também envolve mais apoio técnico, recursos financeiros e investimento. Iniciativas como a *Responsible Data for Children (RD4C)* (https://rd4c.org/), arranjo multissetorial coordenado pelo UNICEF e pelo GOVLAB, podem ser valiosas no sentido de identificar riscos, compreender a dinâmica do melhor interesse para vulneráveis, desenvolver e propor melhores práticas para que os benefícios de uma economia baseada em dados não comprometam o bem-estar de segmentos e indivíduos vulneráveis.**
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	**1) Programa de privacidade (Art. 50 LGPD): Mitigar, prevenir e prover maior controle sobre os riscos envolvidos no tratamento de dados; reduzindo substancialmente os passivos, bem como a chance de sofrer com multas e/ou processos judiciais. Além disso, o programa de governança de dados pode ser uma poderosa ferramenta de marketing, ganhando-se assim a confiança de clientes e parceiros comerciais. Nesse aspecto, as regras de boas práticas e de governança poderão tanto informar PMEs na elaboração de um sólido programa, quanto servir parâmetro de avaliação contínua da**

	robustez do programa em questão.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	**Impactos nos custos: O custo com adequação, implementação e manutenção de um programa de governança de dados pessoais poderá comprometer a viabilidade do próprio negócio, frente à complexidade exigida. Portanto, o incentivo da ANPD na promoção por uma cultura educativa e de prevenção será fundamental**
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	**Responsabilidade civil do controlador PME na cadeia de tratamento** **1. Aspectos ancilares à responsabilidade civil, mas que servem como ferramenta preventiva à violação da LGPD e à ocorrência futura de danos. Podem servir também como instrumento de defesa em processos judiciais para provar medidas adequadas ao risco identificado. Contudo, a avaliação sistemática de riscos, bem como a elaboração do relatório de impacto, pelos controladores de pequeno porte podem ser deficitárias e seriamente comprometidas caso um operador - com peso muito expressivo no mercado e grande número de clientes - se recuse a colaborar de forma mais ativa com as PMEs em questão; seja porque há um temor de revelar informações comerciais a serem aproveitadas por seus concorrentes, seja porque considera que as PMEs têm um poder de pressão e negociação negligenciável. Assim, estender a responsabilidade de forma mais abrangente ao operador pode servir indiretamente como incentivo a um engajamento mais substantial do operador na avaliação sistemática de riscos e na sua prestação satisfatória de informação sobre elementos técnicos no tratamento tais como localização geográfica dos seus servidores. Deste modo, evitar-se-á que todo ônus pese sobre as PMEs.** **Sandbox para startups em proteção de dados** **1. A avaliação sistemática de riscos em startups deve ser realizada de forma contínua com intervalos mais curtos que no caso de empresas tradicionais, considerando-se a natureza extremamente incerta de suas atividades com impactos muitas vezes imprevisíveis.**

Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	**Sandbox para startups em proteção de dados** 1. **Ao se impor um direito à portabilidade e a neutralidade tecnológica como princípio, permite-se mais flexibilidade às startups na escolha de suas ferramentas e na elaboração de seus produtos; podendo-se recorrer inclusive a opções de open source, barateando-se custos e diminuindo-se as barreiras de acesso ao mercado.**
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	**Programa de privacidade (Art. 50 LGPD)** **Comitês setoriais eleitos periodicamente e com representação igualitária de modo a dar voz ativa às PMEs que estejam em comunicação direta com a ANPD, e que sejam governados por um regimento interno definido com a autoridade nacional, com a finalidade de:** 1. **sugerir, inspirar e elaborar regras de boas práticas e de governança;** 2. **avaliar impactos e potencial de contribuição das regras propostas por atores privados, aconselhando a ANPD para reconhecê-las e divulgá-las ou não, em concordância com estes dois elementos.** **Responsabilidade civil do controlador PME na cadeia de tratamento** **Instrumento de soft law: elaborar e publicizar um modelo de contrato para tratamento de dados entre controlador e operador, incluindo cláusulas que exijam um papel mais predominante dos operadores; mitigando assim as assimetrias informacional e negocial, ainda que a LGPD não preveja a formalização por escrito da relação entre os dois agentes de tratamento como é determinado pelo Art. 28(3) RGPD.** **Sandbox para startups em proteção de dados** 1. **Fórum com stakeholders - startups, outros órgãos governamentais, associações de defesa do consumidor, etc - para monitorar potenciais impactos e danos trazidos pelas inovações, e assim, elaborar respostas regulatórias -**

	preferencialmente por meio de normativas da ANPD - de modo célere, eficaz e eficiente.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. 627 CLT	
Art.	

Tomada de Subsídios 1/2021

Joao Araujo Monteiro NetoEIRO [redacted]

seg 01/03/2021 22:40

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

2 anexos

Anexo I da proposta do GETIS ANP.pdf; Contribuição_GETIS_ANPD_PME_010321.pdf;

Prezado(a) Sr(a),

Encaminho a V.Sia a singela contribuição do Grupo de Estudos em Tecnologia, Informação e Sociedade (GETIS) da Universidade de Fortaleza.

Aproveitamos a oportunidade para parabenizar a Autoridade Nacional de Proteção de Dados Pessoais pela louvável iniciativa de abrir espaço para que os mais variados atores da sociedade brasileira possam contribuir para a construção de um ecossistema regulatório de proteção de dados pessoais capaz de proteger os direitos dos titulares ao mesmo tempo que fomenta o desenvolvimento econômico e social.

Ao mesmo tempo que estamos gratos pela oportunidade de colaborar com essas iniciativa aproveitamos para nos colocar à disposição da ANPD para os esclarecimentos necessários sobre nossas sugestões bem como para fomentar os debates que sejam necessários sobre a proteção de dados pessoais em nossa região.

Atenciosamente,

João Araújo Monteiro Neto

Professor do Curso de Direito e Coordenador do GETIS

--

[redacted]

e Aprendendo

<https://g1.globo.com/ce/ceara/especial-publicitario/unifor/ensinando-e-aprendendo/>

<https://g1.globo.com/ce/ceara/especial-publicitario/unifor/ensinando-e-aprendendo/>

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Grupo de Estudos em Tecnologia, Informação e Sociedade – GETIS, Universidade de Fortaleza – UNIFOR (Pesquisadores e alunos envolvidos: João Araújo Monteiro Neto, Alex Renan Galvão, Ana Luísa Schiavo, Iago Capistrano Sá, Ikaro Fontenele, Isabelle Mendes, Victor Coelho)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	A aplicação das regras de proteção de dados pessoais as micro e pequenas empresas é um tema complexo e que demanda cuidadosa atenção dos reguladores uma vez que inadequada calibração da aplicação dos mecanismos regulatórios de proteção de dados pessoais pode sufocar economicamente (aumento do custo de funcionamento) e operacionalmente (aumento de atividades e controles administrativos) os pequenos e médios negócios. Ao mesmo tempo, a falta de *enforcement* das medidas previstas no sistema regulatório pode levar a um enfraquecimento do grau de proteção aos titulares quanto sujeitos à operações de tratamento conduzidas por estes atores, o que, coloca não somente as operações desses atores num patamar de maior vulnerabilidade e risco, mas também todo o ecossistema de proteção e dados pessoais, uma vez que o dado pessoal protegido pelas grandes empresas também circulará, de forma mais vulnerável nas pequenas e médias, o que fragiliza todo o ecossistema de proteção de dados pessoais. Nesse contexto, um outro fator que deve ser observado é a caracterização de micro e pequena empresa no cenário de tratamento de dados pessoais, posto que os critérios econômicos e de quantidade de funcionários, não

	permitem uma correta compreensão do nível de risco aos titulares que as atividades de tratamento desempenhadas pelas micro, pequena e média empresas podem oferecer. Dessa forma, respeitando a objetividade solicitada pela chamada pública apontamos como os principais desafios relacionados ao tema os seguintes pontos: A) Adequada caracterização de pequena empresa no ecossistema de tratamento de dados pessoais. Necessidade de olhar multidimensional para a correta caracterização de uma empresa de pequeno porte que trate dados pessoais e possa ser isenta ou ter algumas obrigações flexibilizadas. Faturamento e quantidade de funcionários não podem ser considerados como vetores isolados de classificação. Deve-se observar critérios relacionados a complexidade da operação de dados pessoais alvo do negócio e também a sensibilidade dos dados pessoais tratados por esses atores; B) Calibragem do processo de flexibilização-simplificação das medidas técnicas e organizacionais necessárias à proteção de dados pessoais quando aplicadas à PMEs que não como por exemplo, ROPAS, RIPDs, LIAs, E
Existem sugestões para endereçamento do problema?	Sugerimos a indicação de critério que leve em consideração a complexidade do tratamento de dados pessoais pela empresa. O conceito da complexidade do tratamento dos dados pessoas deve levar em consideração dois grandes vetores: 1. O risco de atividade de tratamento (Deve ser calculado em observância as orientações da Agência Europeia de CiberSegurança – ENISA (Ver guidelinesfor SMEs on the security of personal data processing); 2. Complexidade da operação de tratamento: Indicamos abaixo, com base nas indicações da ENISA, uma modelagem inicial do fator de complexidade da operação de tratamento de dados pessoais por PMEs:

Dimensionamento da Complexidade do Tratamento dos Dados Pessoais:

A definição da complexidade das operações de tratamento realizadas no escopo da PME deve observar 4 dimensões relacionadas ao tratamento. Para simplificar esse processo, várias perguntas de avaliação, tendo como base o framework desenvolvido pela ENISA, são sugeridas. As áreas de avaliação são:

A. Natureza dos dados e da operação de tratamento de dados pessoais;
B. Recursos técnicos de sustentação ao tratamento dos dados pessoais;
C. Processos e pessoas relacionadas ao tratamento de dados pessoais;
D. Atividade negocial e escala do tratamento;

A tabela abaixo indica as questões relacionadas à avaliação da complexidade das atividades de tratamento para cada segmento apresentado acima:

A. NATUREZA DOS DADOS E DA OPERAÇÃO DE TRATAMENTO DE DADOS PESSOAIS	
1	Qual a natureza dos dados pessoais tratados?
2	A operação de tratamento envolve dados de crianças e adolescentes?
3	A operação de tratamento envolve decisões automatizadas?
4	A operação de tratamento envolve volumes significativos de dados pessoais?
5	A operação de tratamento envolve processos inovadores ou disruptivos?

B. RECURSOS TÉCNICOS APLICADOS AO TRATAMENTO DOS DADOS PESSOAIS	
6	Alguma parte do tratamento de dados pessoais é realizada pela Internet?
7	É possível fornecer acesso a um sistema interno de tratamento de dados pessoais através da Internet (por exemplo, para determinados usuários ou grupos de usuários)?
8	O sistema de tratamento de dados pessoais está interconectado a outro sistema ou serviço de TI externo ou interno?
9	Existe trânsito internacional de dados pessoais?

10	Existem garantias a confidencialidade, integridade e disponibilidade dos sistemas envolvidos no tratamento?

C. PROCESSOS E PESSOAS RELACIONADAS AO TRATAMENTO DE DADOS PESSOAIS	
11	As funções e responsabilidades em relação ao tratamento de dados pessoais são vagas ou estão claramente definidas?
12	Os processos envolvem tecnologias ou práticas de difícil rastreamento ou auditagem?
13	O tratamento de dados pessoais é realizado por um número não definido de funcionários?
14	Alguma parte da operação de tratamento de dados é realizada por um contratado / terceiro (operador)?
15	Existe utilização de processos de mineração e enriquecimento de dados pessoais?

D. ATIVIDADE NEGOCIAL E ESCALA DO TRATAMENTO	
16	A atividade de tratamento pode gerar dano as liberdades fundamentais, a vida ou a saúde dos titulares?
17	A atividade negocial está sujeita a alguma autoridade regulatória ou a mecanismos de controle específicos?
18	A atividade de tratamento explora alguma área ainda não regulada pela ANPD?
19	As operações de tratamento dizem respeito a um grande volume de indivíduos e/ou dados pessoais?
20	As operações de tratamento dizem respeito a dados ou processos de grande sensibilidade?

As Tabelas 1 e 2 (abaixo apresentadas) devem ser utilizadas para documentar e evidenciar a análise da complexidade do tratamento para cada área de avaliação e, consequentemente, indicar o valor final:

ÁREA DE AVALIAÇÃO	PROBABILIDADE	
	NÍVEL	PONTUAÇÃO
Natureza dos dados e da operação de tratamento de dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Recursos técnicos de sustentação ao tratamento dos dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Processos e pessoas relacionadas ao tratamento de dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Atividade negocial e escala do tratamento	☐ Baixa	1
	☐ Média	2
	☐ Alta	3

(Tabela 1)

RESUMO GLOBAL DE COMPLEXIDADE	NÍVEL DE COMPLEXIDADE
4-5	**Baixa**
6-8	**Média**
9-10	**Alta**
10-12	**Altíssima**

(Tabela 2)

Tabela de apresentação final do grau de complexidade da PME em relação ao tratamento de dados pessoais.

Uma vez caracterizada como PME dentro dos fatores já existentes na legislação brasileira, deve ser realizado o teste de complexidade para aferir em qual categoria de tratamento a PME se enquadra e quais medidas de isenção-flexibilização ela faria jus.

		COMPLEXIBILIDADE			
		BAIXA	MÉDIA	ALTA	ALTÍSSIMA
RISCO	BAIXO				
	MÉDIO				
	ALTO				

PME DE PEQUENA COMPLEXIDADE		PME DE MÉDIA COMPLEXIDADE		PME DE ALTA/ALTÍSSIMA COMPLEXIDADE	

(Tabela 3)

A depender da caracterização da PME ela poderá ser beneficiada com:

a) PME com tratamento de pequena complexidade: Isenção de algumas medidas de controle como EPD e RIPD, e simplificação de outras como ROPA, etc;

b) PME com tratamento de média complexidade: Flexibilização de algumas medicas como o compartilhamento de EPDs e simplificação de outras como o RIPD;

c) PME com tratamento de alta e altíssima complexidade: Nenhuma exclusão.

	Por fim sugere-se que a exemplo da Agência Espanhola de Proteção de Dados Pessoais seja desenvolvido um conjunto de mecanismos de apoio às PMEs. Dentre as inúmeras possibilidades indicam-se as seguintes: i. Criação de ferramenta de autodiagnostico de adequação à LGPD; ii. Disponibilização de ferramenta de avaliação de riscos simplificadas; iii. Disponibilização de ferramenta de avaliação de legítimo interesse simplificada; iv. Disponibilização de plataforma de Registro de Atividade de Tratamento (ROPA); v. Disponibilização de banco de informações contendo modelos de cláusulas contratuais e avisos de privacidade; vi. Disponibilização de ferramenta de geração de políticas de privacidade e termos de usos simplificados; vii. Fomento a construção de redes de compartilhamento de EPDs em atores estratégicos como entidades associativas de PMEs ou Universidades. Sugere-se por fim o estabelecimento de programa de apoio às PMEs nas áreas de segurança da informação e proteção de dados pessoais em Universidade públicas e privadas.
Quais são as oportunidades relacionadas ao tema?	Possibilidade de estimular atores setoriais como aqueles pertencentes ao sistema “S” (SENAI, SEBRAE, etc), as Federações representativas de áreas de negócio como a Federação das Indústrias, e as Câmaras Negocias com as Câmaras de Dirigentes Lojista a desenvolverem programas de apoio à adequação da LGPD das PMEs pertencentes aos seus ecossistemas.
Quais são as experiências internacionais sobre o tema?	Dentre as experiências internacionais pesquisadas, se destacam as da Agencia Española de Protección de Datos Personales (AEPD), da Information Commissioner’s Office (ICO), do Office of the Australian Information Commissioner (OAIC) e da European Commission. **2.1. Agencia Española de Protección de Datos Personales (AEPD)** A AEPD disponibiliza uma plataforma gratuita e de simples acesso chamada “Facilita RGPD”: ferramenta de auxílio aos agentes de tratamento de dados pessoais, com a geração automática de um Registro de Operações de Tratamento de Dados.

	A ferramenta, que pode ser acessada em https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd, faz uma série de questionamentos sobre o modelo de negócio da empresa e o tratamento de dados pessoais em si, sendo eles: • Setor ao qual a organização pertence; • Tipos de dados que a organização trata; • Se, dentre os dados tratados, há dados sensíveis; Há respostas prontas para os três questionamentos acima, e, como última opção, "nenhuma das anteriores". Dependendo da marcação, a resposta pode ser: 1) Caso seja marcada alguma das alternativas com respostas preestabelecidas: "com os dados que você forneceu, este programa não é adequado para você, pois sua empresa não atende aos requisitos para seguir [no uso da ferramenta]. Você deve realizar uma análise de risco". E então a ferramenta encerra o seguimento. 2) Caso não seja marcada nenhuma das alternativas com respostas preestabelecidas: "você respondeu negativamente a todas as questões anteriores, portanto, pode-se entender que os tratamentos realizados por sua entidade acarretam, a priori, um baixo nível de risco para os direitos e liberdades das partes interessadas e, portanto, estariam à disposição de usar o seguinte programa". Assim, passa-se ao preenchimento de informações sobre a empresa para gerar documentos automaticamente adaptados à organização, que são: • Nome da empresa; • Endereço completo da empresa; • Número de Identificação Fiscal; • Telefone; • Endereço de e-mail; • Descrição da atividade; • Endereço de e-mail para o exercício de direitos.

	A equipe de pesquisadores preencheu informações simuladas nos campos mencionados acima, para que a operação pudesse prosseguir. A seguir, são feitos novos questionamentos – e, em sendo afirmativas as respostas, outras perguntas surgirão, a fim de ter especificações. • Sua organização trata dados pessoais de clientes (pessoas físicas)? (refere-se aos dados pessoais das pessoas com quem você mantém uma relação comercial); • Sua organização trata dados pessoais de potenciais clientes (pessoas físicas)? • Sua organização trata dados pessoais de empregados? • Sua organização trata dados pessoais de candidatos? • Sua organização trata dados pessoais de fornecedores (pessoas físicas)? • Sua organização captura imagens usando câmeras de vigilância por vídeo para fins de segurança? • Sua organização possui empresas terceirizadas que prestam serviços como manutenção do seu site, desenvolvimento de programas de computador, provedor de e-mail, hospedagem, serviço de limpeza, serviço de vigilância por vídeo ou outros? Com isso, o programa é finalizado, e documentos em formato editável são disponibilizados para download. Ainda aparece o seguinte recado: LEMBRE-SE, embora sejam oferecidos a você os documentos mínimos essenciais para estar em posição de cumprir o Regulamento de Proteção de Dados, você também deve realizar as seguintes ações: 1. Inclua as cláusulas informativas nos formulários de solicitação de informações, seja por meio de formulários em papel ou por meio do seu site. 2. Implementar as medidas técnicas e organizacionais indicadas no documento correspondente.

	3. Reveja os contratos que você tem atualmente e inclua as cláusulas contratuais e assine-os na última página. 4. Prepare os contratos que ainda não tem e inclua também as cláusulas contratuais e assine-as na última página. 5. Proteja e mantenha todos os documentos atualizados. 6. Não se esqueça que não deve enviar nada à Agência Espanhola de Proteção de Dados, apenas deve dar-lhes se for solicitado. 7. Lembre-se que a Agência Espanhola de Proteção de Dados não armazena as informações que você inseriu nesta ferramenta. O modelo de documento preenchido pela equipe para demonstração segue em anexo. **2.2. Information Commissioner's Office (ICO)** O ICO disponibiliza, em seu site, informações relevantes para pequenas empresas (ICO, 2021. Página Principal. Disponível em: <https://cy.ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/whats-new/blogs/ico-helpline-advisors-share-their-top-data-protection-tips-for-small-organisations/>. Acesso em: 28 de fevereiro de 2021). A partir disso, mesmo que não tenha nenhum domínio sobre o assunto, o empresário deve ser instigado a fazer uma avaliação da situação de seu negócio respondendo inicialmente as seguintes questões simples: 1. Você sabe exatamente quais os tipos de dados pessoais você tem sobre as pessoas e onde eles estão salvos? 2. Você sabe para que está usando essa informação? 3. Você sabe por quanto tempo mantém ou irá manter essa informação? 4. Você disse às pessoas donas dos dados por que você precisa desses dados? 5. Você tem certeza absoluta que está mantendo esses dados de forma segura?

De acordo com o ICO, o comportamento dos pequenos empresários deve girar em torno do básico. Primeiramente, é fundamental que eles entendam por qual razão precisam dos dados, onde usam e para onde serão enviados. Em seguida, se deve fazer uma análise simples de quais dados são cruciais para o serviço prestado e quais não são e não necessitam ser colhidos. Feito isso, há de se adquirir o hábito de informar aos clientes a finalidade da coleta desses dados.

2.3. Office of the Australian Information Commissioner (OAIC)

O OAIC fornece uma Lista de Verificação de Privacidade para Pequenas Empresas, a qual vale a pena conferir:

- Sua pequena empresa lida com informações pessoais?
- Sua pequena empresa teve um faturamento anual de mais de US $ 3.000.000 em qualquer exercício financeiro desde 2002?
- A sua pequena empresa comercializa informações pessoais?
- Sua pequena empresa comercializa informações pessoais sem o consentimento do indivíduo e sem ser exigida ou autorizada por lei?
- A sua pequena empresa é prestadora de serviços de saúde?
- A sua pequena empresa está relacionada a uma corporação maior sujeita à Lei de Privacidade?
- A sua pequena empresa é uma prestadora de serviços contratada pelo Governo?
- Você é uma entidade relatora ou um agente autorizado de uma entidade relatora de acordo com a Lei de Combate à Lavagem de Dinheiro e Financiamento ao Terrorismo de 2006 (Lei AML / CTF) ou seus regulamentos ou regras?
- A sua pequena empresa opera um banco de dados de locação residencial?
- A sua pequena empresa opera com relatórios de crédito?
- A sua pequena empresa optou voluntariamente pela Lei de Privacidade?

(OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. OAIC. https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/ Acesso em: 28 de fevereiro de 2021).

2.4. European Commission

	A European Commission, acerca do registro das atividades de tratamento, ressalta que esse registro só deve ocorrer em casos especiais, sendo eles: a) O tratamento efetuado possa resultar em risco para os direitos e liberdades do titular dos dados; b) O tratamento não seja ocasional; c) O tratamento abranja as categorias especiais de dados pessoais ou sejam referentes a dados pessoais relativos a condenações penais e infrações. (EUROPEAN COMMISSION. EC. EUROPA, 2018. <https://ec.europa.eu/justice/smedataprotect/index_en.htm>. Acesso em: 28 de fevereiro de 2021). Isso em atenção ao art. 30º (dispõe sobre a estrutura do registro), 5, do RGPD, que diz: 5. As obrigações a que se referem os n.os 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.o
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Como mencionado acime entendemos que o grau de complexidade da operação de tratamento deve orientar o processo de avaliação das PMEs e não somente os aspectos tradicionais do faturamento e da quantidade de funcionários. Ver Anexo I.
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)?	**Nada a contribuir**
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	Como apontado anteriormente, a ausência de mecanismos de simplificação-flexibilização pode aumentar a burocracia e o custo operacional dos PMEs.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	**Nada a contribuir**

Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	**Nada a contribuir**
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?	**Nada a contribuir**
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	**Nada a contribuir**
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	**Nada a contribuir**
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	**Nada a contribuir**
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	**Nada a contribuir**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Nada a contribuir	

Dimensionamento da Complexidade do Tratamento dos Dados Pessoais:

A definição da complexidade das operações de tratamento realizadas no escopo da PME deve observar 4 dimensões relacionadas ao tratamento. Para simplificar esse processo, várias perguntas de avaliação, tendo como base o framework desenvolvido pela ENISA, são sugeridas. As áreas de avaliação são:

A. Natureza dos dados e da operação de tratamento de dados pessoais;
B. Recursos técnicos de sustentação ao tratamento dos dados pessoais;
C. Processos e pessoas relacionadas ao tratamento de dados pessoais;
D. Atividade negocial e escala do tratamento;

A tabela abaixo indica as questões relacionadas à avaliação da complexidade das atividades de tratamento para cada segmento apresentado acima:

A. NATUREZA DOS DADOS E DA OPERAÇÃO DE TRATAMENTO DE DADOS PESSOAIS	
1	Qual a natureza dos dados pessoais tratados?
2	A operação de tratamento envolve dados de crianças e adolescentes?
3	A operação de tratamento envolve decisões automatizadas?
4	A operação de tratamento envolve volumes significativos de dados pessoais?
5	A operação de tratamento envolve processos inovadores ou disruptivos?

B. RECURSOS TÉCNICOS APLICADOS AO TRATAMENTO DOS DADOS PESSOAIS	
6	Alguma parte do tratamento de dados pessoais é realizada pela Internet?
7	É possível fornecer acesso a um sistema interno de tratamento de dados pessoais através da Internet (por exemplo, para determinados usuários ou grupos de usuários)?
8	O sistema de tratamento de dados pessoais está interconectado a outro sistema ou serviço de TI externo ou interno?
9	Existe trânsito internacional de dados pessoais?
10	Existem garantias a confidencialidade, integridade e disponibilidade dos sistemas envolvidos no tratamento?

C. PROCESSOS E PESSOAS RELACIONADAS AO TRATAMENTO DE DADOS PESSOAIS	
11	As funções e responsabilidades em relação ao tratamento de dados pessoais são vagas ou estão claramente definidas?
12	Os processos envolvem tecnologias ou práticas de difícil rastreamento ou auditagem?
13	O tratamento de dados pessoais é realizado por um número não definido de funcionários?
14	Alguma parte da operação de tratamento de dados é realizada por um contratado / terceiro (operador)?
15	Existe utilização de processos de mineração e enriquecimento de dados pessoais?

D. ATIVIDADE NEGOCIAL E ESCALA DO TRATAMENTO	
16	A atividade de tratamento pode gerar dano as liberdades fundamentais, a vida ou a saúde dos titulares?
17	A atividade negocial está sujeita a alguma autoridade regulatória ou a mecanismos de controle específicos?
18	A atividade de tratamento explora alguma área ainda não regulada pela ANPD?
19	As operações de tratamento dizem respeito a um grande volume de indivíduos e/ou dados pessoais?
20	As operações de tratamento dizem respeito a dados ou processos de grande sensibilidade?

As Tabelas 1 e 2 (abaixo apresentadas) devem ser utilizadas para documentar e evidenciar a análise da complexidade do tratamento para cada área de avaliação e, consequentemente, indicar o valor final:

ÁREA DE AVALIAÇÃO	PROBABILIDADE	
	NÍVEL	PONTUAÇÃO
Natureza dos dados e da operação de tratamento de dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Recursos técnicos de sustentação ao tratamento dos dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Processos e pessoas relacionadas ao tratamento de dados pessoais	☐ Baixa	1
	☐ Média	2
	☐ Alta	3
Atividade negocial e escala do tratamento	☐ Baixa	1
	☐ Média	2
	☐ Alta	3

(Tabela 1)

RESUMO GLOBAL DE COMPLEXIDADE	NÍVEL DE COMPLEXIDADE
4-5	**Baixa**
6-8	**Média**
9-10	**Alta**
10-12	**Altíssima**

(Tabela 2)

Tabela de apresentação final do grau de complexidade da PME em relação ao tratamento de dados pessoais.

Uma vez caracterizada como PME dentro dos fatores já existentes na legislação brasileira, deve ser realizado o teste de complexidade para aferir em qual categoria de tratamento a PME se enquadra e quais medidas de isenção-flexibilização ela faria jus.

		COMPLEXIBILIDADE			
		BAIXA	MÉDIA	ALTA	ALTÍSSIMA
RISCO	BAIXO				
	MÉDIO				
	ALTO				

PME DE PEQUENA COMPLEXIDADE		PME DE MÉDIA COMPLEXIDADE		PME DE ALTA/ALTÍSSIMA COMPLEXIDADE	

(Tabela 3)

Tomada de Subsídios 1/2021

João Peres[redacted]

dom 28/02/2021 21:09

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

2 anexos

Anexo1-TSIOT.pdf; Contribuicoes - TOMADA DE SUBSÍDIOS Nº 1 2021 -Tudo-sobre-IoT+AIR 01.pdf;

Prezados Senhores(as).
Em nome da comunidade **“Tudo-sobre-IoT”** e demais colaboradores, estamos encaminhando em anexo nossas contribuições sobre a Tomada de subsídios 01/2021 da ANPD, composta por dois documentos 1) Contribuições... 2)Anexo1...

Caso haja qualquer dúvida, ou mecessitem maiores informações, estamos ao inteiro dispor.

Att.

João Peres
[redacted]
NEWKOMP
KOMP SECURITY BRAZIL
https://www.komp.com.br
[redacted]

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Tudo-sobre-IoT + KOMP Security, Uberconsult® e outras

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável às microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

OBS.: Utilizamos o acrônimo **EPPs** para designar genericamente; microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
1- Quais são os desafios/problemas regulatórios relacionados ao tema?	**Os grandes Desafios que identificamos:** 1- **Qualificação do porte das organizações brasileiras –** Acreditamos que a Lei complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte e complementos deva ser considerada, no entanto "não" se faz adequada para o enquadramento de empresas quanto ao porte para atendimento aos ditames da Lei 13.709:2018, mesmo considerando o Artigo 55J –XVIII da Lei nº 13.853, de 8 de julho de 2019 pois, o ***enquadramento deveria ser realizado com base no volume, tipo de dados (regular, sensível, crianças e adolescentes), criticidade, local e frequência de tratamento de dados pessoais*** que uma empresa necessita para operar. Como reflexão, encontramos na prática, grandes organizações operando em B2B, tratando dados pessoais comerciais de baixa criticidade e em volumes menores do que muitas empresas de muito pequeno porte. -- Vide fundamentação e justificativas no "Anexo 1" Documento: Anexo1-TSIOT.pdf

	2- Considerar aspectos culturais, sociais e econômicos brasileiros – Apesar de serem temas conhecidos, realçamos a necessidade de entender o indicador chave **IPCLBrasil** - (Índice de percepção do cumprimento de Leis no Brasil - (compliance with the law)), que necessitaria ser atualizado e focado agora para a LGPD em 2021. Compreender a efetiva "resistência" de empresários brasileiros e seus reais motivos, em adotar os requerimentos legais da LGPD, passa a ser fundamental para o planejamento estratégico de ações que possam acelerar o convencimento e a adequação, sem criar os estigmas das sanções. Nesta mesma linha, é importante compreender o problema da não adesão à LGPD, considerando a inércia similar ocorrida na União Europeia com a GDPR, no seu primeiro e segundo ano, após sua entrada em vigor em 25 de maior de 2018. -- Vide fundamentação e justificativas no "Anexo 1". **3- Práticas metodológicas e normativas em uso cotidiano nas empresas nacionais** – Entendemos que infelizmente no nosso país a adoção às Normas Internacionais (ISO) e melhores práticas possui baixa aderência. No campo e na prática, observamos que padrões fundamentais como a Norma NBR ISO/IEC 27002 (código de práticas e controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação), traduzida e publicada como ISO 17799:2000 e atualizada oficialmente para ISO/IEC 27002 em julho 2007, até hoje é muito pouco conhecida e praticada nas empresas de todos os portes. Aqui o grande desafio é compreender e planejar ações motivacionais que possam sensibilizar empresários na busca de adoção de padrões e melhores práticas mínimas necessárias para aumentar a competitividade das nossas empresas e para o crucial atendimento à Privacidade e Proteção de Dados. -- Vide fundamentação e justificativas no "Anexo 1". **4- Estabelecer Níveis de Maturidade a serem alcançados** – Entendemos ser fundamental estudar e estabelecer patamares a serem alcançados, tanto na adequação à LGPD, Governança de Dados e Cultura de Privacidade e Proteção de Dados e a evolução dos conhecimentos dos Encarregados em um horizonte de tempo pré-definido. Aqui recomendamos uma adaptação dos modelos internacionais CMMi (Capability Maturity Model Integration) e PCMM (People Capability Maturity Model). -- Vide fundamentação e justificativas no "Anexo 1".

	5- Planejamento Estratégico de Programas de Motivação e Alcance – Entendemos que se faz necessário priorizar o planejamento de inciativas como equacionar campanhas públicas para "Agentes de Tratamento de Dados". Sugerimos aqui algumas e as detalhamos no Anexo correspondente – por exemplo: **a)** campanha de divulgação "**Só não cumpre a LGPD quem não quer**" – para atender as empresas qualificadas como EPP (empresas de Pequeno Porte para a LGPD). No Portal da ANPD poderia haver um "Guia de Melhores Práticas" para esse perfil de empresa, como a Autoridade de Proteção de Dados Inglesa - ICO (Information Commissioner's Office) divulga em sua página web "Data protection advice for small organisations". https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/ **b)** Outra hipótese seria uma campanha ofertando um SELO ANPD "**Empresa Colaboradora ANPD – fomentando a Cultura da Privacidade e Proteção de Dados**", para as empresas investirem ou cooperarem em ações de aculturamento de outras organizações menores que se inscrevam graciosamente em seus Portais de Conhecimento EAD. **c)** Como terceira hipótese, a produção da campanha e SELO ANPD "**Empresa Aderente a LGPD - Self Certified**", pode ser muito motivador - recomendamos estabelecer parâmetros de requerimentos objetivos e práticos que possam ser auditáveis e efetivamente alcançados pelas empresas. Para atender o proposto nesta terceira hipótese **c)**, entendemos que algumas práticas normatizadas em outras áreas, como é o caso do padrão estabelecido pelas Normas de "Autodeclaração de Conformidade", tratada nas normas internacionais ISO/IEC 17050:2004-1 e ISO/IEC 17050:2004-2. A parte 1 da 17050 foi desenvolvida com o objetivo de fornecer requisitos gerais para a Declaração de Conformidade do Fornecedor (SDoC, na sigla em inglês), possam servir de embasamento no caso da LGPD. Sabemos que o tema "Certificação" é polêmico e conhecemos as implicações e todas as questões de "Acreditação Oficial", através de delegações do INMETRO e alinhamentos internacionais, no entanto, avaliações de terceira parte estão ganhando

	força no mundo contemporâneo e passaram a ser um instrumento de incentivo a conformidade e gerador de novos empregos. – vide: http://inmetro.gov.br/Credenciamento/index.asp Fundamentação e justificativas no “Anexo 1”.
2 - Existem sugestões para endereçamento do problema?	**Várias – em textos anexos do Anexo 1.**
3 - Quais são as oportunidades relacionadas ao tema?	**1) Para a ANPD -** Atender aos requerimentos do Artigo 55-j da Lei 13.853, relacionados aos incisos VI, VII, VIII, XVIII e XXIV, entre outros. **2) Para os Titulares de dados –** Com a devida divulgação de ações efetivas da ANPD, ampliar a cultura popular da Privacidade e da necessária Proteção de Dados Pessoais, permitindo maior interatividade social e redução dos riscos associados. **3) Para empresas EPPs –** Com o resultado do Planejamento, a ANPD poderá promover programas de conscientização, implementação de estruturas de Apoio e Campanhas de divulgação, conforme proposto no “ANEXO 1”. **4) Para as empresas de Consultoria e Prestação de Serviços –** Considerando um regramento complementar para as EPPs produzido pela ANPD, as empresas de Consultoria e Prestação de serviços, no suporte ou implementação da LGPD, poderão ofertar ao mercado novas alternativas de soluções, em muitos casos até padronizadas, que sejam mais efetivas e econômicas. **5) Para as grandes empresas Patrocinadoras/Apoiadoras** - Acreditamos que através de campanhas para busca de apoio e parcerias com grandes empresas nacionais e multinacionais, a ANPD poderá promover a disseminação da cultura de Privacidade e Proteção de Dados, chegando à população e aos empresários em geral das EPPs.
4 - Quais são as experiências internacionais sobre o tema?	Em todos os países que pesquisamos, com base na “**unctad.org**” (Assembleia Geral da ONU e ao Conselho Econômico e Social – congrega 195 nações), a grande maioria (128) possui preocupação em flexibilizar as Normas de Privacidade e Proteção de Dados pessoais, no entanto, **muito pouco foi realmente realizado até o momento**. Entendemos que existem manifestações em textos legais, como no caso da LGPD, mas a flexibilização de regras compromete a “Segurança dos Titulares de Dados”, que é o objetivo chave das legislações no mundo. Por outro lado, incentivar as pequenas empresas na busca da adequação a LGPD, permitirá uma evolução gradativa de amadurecimentos de processos operacionais chaves, onde a Prevenção por identificação de Riscos, a Segurança da

	Informação, a Conformidade Regulatória inclusive “Accountability”, dos processos de identificação e respostas a incidentes, entre outros, deverão ser incorporados naturalmente. A LGPD requerida e fomentada trará um grande benefício para incentivar e promover a inovação nas empresas e no país. Algumas poucas ações pontuais na EU. Principais flexibilizações (não foram todos os países que adotaram): • Isenção do RoPa; • Isenção do DPIA; • Isenção do DPO; • Isenção ou redução de Taxas.
5 - Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	O enquadramento do porte dos Agentes de Tratamento de Dados Pessoais deveria ser estabelecido com base no **volume, tipo (regular, sensível, crianças e adolescentes) criticidade, local e frequência de tratamento de dados pessoais,** por eles realizados. Poderia ser criado um “**Quadro de Avaliação de Porte Organizacional On-line**” (web), através de um questionário interativo, onde as empresas poderiam entender o seu enquadramento perante à LGPD. Considerando os parâmetros usados por instituições como IBGE, ANVISA, BNDES, entre outras, que de certa forma estão alinhadas com as práticas da União Europeia, com foco em “Quantidade de Colaboradores e Faturamento Anual” entendemos que para a LGPD deveria também ser **adicionado para uma melhor avaliação de porte, parâmetros** como: a) **Quantidade (volume: baixo, médio, alto)** de Dados Pessoais tratados pela empresa; Quantidade de Bancos de Dados em uso, etc; b) **Tipos de Dados** Pessoais disponíveis – classificação em 3 classes (regular, sensíveis e de Crianças e Adolescentes); c) **Nível de Criticidade** – i) % de importância desses dados “por tipo” para os negócios; ii) % de riscos desses dados “por tipo” para os Titulares; d) **Local** de armazenamento e tratamentos de dados pessoais i) nas instalações da própria empresa; ii) em datacenter terceirizado no Brasil; iii) em nuvem pública, hibrida ou multinuvens, com armazenamento e ou tratamento no Brasil, armazenamento e Tratamento fora do país; e) **Frequência de tratamento** 1) contínuo; 2) diário; 3) semanal; 4) quinzenal; 5) mensal; 6) trimestral; 7) semestral; 8) anual; 9) especifique em detalhes.

	Importante lembrar: Alguns MEIs que disparam e-mail marketing para terceiros, tratam mais dados pessoais do que grandes empresas.
6 - 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)?	A interpretação da GDPR no início foi polêmica quanto ao porte organizacional, onde o parâmetro empresas com menos de 250 colaboradores poderiam estar isentas. Mas logo o problema foi resolvido e entendemos que flexibilização para agentes de tratamento de dados de pequeno porte foi quase nula. Alguns países possuem Guias de orientação para as pequenas empresas, como instrumento didático e em muitos casos fornecem templates de documentos.
7- Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	Entendemos que a grande maioria das empresas que possam ser consideradas de pequeno porte perante a LGPD, não possuem condições, via de regra, para que sozinhas possam realizar um inventário de dados e o registro de operações conforme o alinhamento internacional RoPA (Record of Processing Activities) requerido na GDPR, inclusive para identificar os tipos de dados pessoais tratados, a atribuição de bases legais de tratamento, para atendimento correto das solicitações dos titulares de dados, para demonstrar conformidade, para cumprimento de princípios da Lei (transparência, responsabilização) e a especificação da aplicação dos controles corretos de segurança, de forma a atender eventual fiscalização da ANPD. Da mesma forma, entendemos que o devido registro das atividades de tratamento de dados pode ser base para qualquer programa de GD “Governança de Dados”, mas estas práticas e técnicas de GD, são totalmente ausentes e até desconhecidas pela grande maioria das nossas empresas. Aqui sugerimos praticar algo similar ao previsto no art. 30 (5) do Regulamento Europeu: - **estarão desobrigadas** de realizar esses registros (Record of Processing Activities) as instituições que empregam menos de 250 pessoas, não realizam processamento de alto risco, nem de categorias especiais de dados e antecedentes criminais, e realizam processamento ocasional. Os critérios são cumulativos. É importante esclarecer que na EU o artigo 30 (5) do GDPR não foi aceito por todos os países, como é o caso de Portugal, que exige das pequenas empresas essa atividade, no entanto, estabeleceu uma planilha modelo para que as organizações operem. – veja em: https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

	A fundamentação da CNPD de Portugal é que uma pequena empresa possui colaboradores e processa dados destes regularmente para folha de pagamento mensal. Caso a ANPD opte por manter o "Registro de Operações", sugerimos simplificar os requerimentos e adotar uma planilha como modelo brasileiro para as EPPs.
8 - Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Entendemos que a nomeação de um "Encarregado ou DPO" em empresas que de fato sejam de pequeno porte perante a LGPD seja desnecessária pelos seguintes fatos: 1) Destacar ou contratar algum colaborador para assumir esse cargo seria demais oneroso; 2) As Certificações de DPO disponíveis no mercado com cursos com até 60 horas de aulas, de fato, não conseguem formar bons profissionais capazes de realmente atender os requerimentos da LGPD e da ANPD e almejarem elevados salários; 3) A responsabilidade de atender as demandas da ANPD e dos Titulares de Dados poderia ser de um dos sócios ou executivos da organização, ou mesmo um designado que acumule atividades. Essa pessoa indicada deveria ter a obrigação de fazer por exemplo, dois cursos gratuitos da EV.G (Escola Virtual gov.br - Enap) curso 1- Introdução à Lei Brasileira de Proteção de Dados Pessoais; e curso 2) Proteção de Dados Pessoais no Setor Público – apresentando os certificados para se isentarem de contratar um DPO - reciclagem obrigatória. Outra opção seria essas empresas contratarem serviços de empresas especializadas, a baixo custo como "DPO-as-Service" compartilhado. Entendemos as velhas recomendações de segregação de funções, já preconizadas pela BS7799 e ainda prevalecendo na ISO/IEC-27701, onde indica que possa haver conflitos de interesses dos diretores e donos da empresa em atuação como DPO – a função exige independência. Mas ponderando, a classe de MEI (quase 10 milhões de CNPJs) não podem atender "nomear encarregado", porque trabalham só ou no máximo podem ter um empregado.
9 - Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Com base em nossa proposta de qualificação de empresas de pequeno porte para a LGPD, não faz sentido ser exigido o relatório RIPD ou DPIA, até porque essas organizações poderão estar desobrigadas de realizar o registro de operações de tratamento de dados por não realizam processamento de alto risco, nem de categorias especiais de dados e antecedentes criminais e realizam processamento ocasional, se houver alinhamento internacional.

10 - 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?	Acreditamos que empresas com CNPJ enquadradas como EPPs, inclusive "startups" ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, que declarem tratar dados sensíveis, seja em qualquer volume ou periodicidade, ou realizem transferências internacionais de dados, não devam ser consideradas empresas de pequeno porte para a LGPD. Portanto, estas deverão atender de forma integral ao estabelecido na Lei, não se aplicando qualquer flexibilização.
11 - Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	A grande maioria das pequenas organizações de fato, sequer sabem o significado de Governança e Gestão de Dados. Acreditamos que de uma certa forma, adquirir gradativamente a cultura de Governança de Dados, seja muito salutar para as pequenas organizações. Por outro lado, acreditamos ser inviável implementar um programa de Governança de Dados, no atual nível de maturidade desse porte de empresa, inclusive por questões econômicas e culturais, no momento.
12 - Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	A maioria das EPPs não possuem uma PoSIC (Política de Segurança da Informação) ou ações de melhores práticas nesse tema. Da mesma forma estão muito longe de conhecer os requerimentos do sistema de gestão de privacidade da informação (SGPI) apresentado pela norma ISO/IEC 27701:2019. Essas organizações necessitam urgente, evoluírem e adotarem melhores práticas para prevenção – operação e reação em detectar, relatar e investigar violações de dados, assim que acontecerem – sem isso é inviável atender e divulgar violações em 72 horas como proposto na GDPR. Muitas empresas no Brasil levam meses para descobrirem um vazamento de dados. Acreditamos que a ANPD deveria manter essa exigência para todas as organizações independente do porte, até para incentivar a sustentação, evolução e a capacidade competitiva destas, além de garantir a perenidade.
13 - Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	A avaliação de riscos deveria ser uma atividade constante e corriqueira nas empresas de todos os portes. Trata-se de uma ferramenta de gestão indispensável nas organizações. Sua adoção pode motivar as organizações a utilizarem também outros instrumentos de gestão de grande relevância. Acreditamos que o modelo genérico apresentado no Manual de Gestão de Riscos do TCU (maio 2018), possa ser ajustado para aculturar as EPPs. Disponível em 25/02/21: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=FF8080816364D79801641D7B3C7B355A

14 -Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	Não há como garantir portabilidade, sem uma boa gestão das bases de dados e padrões estabelecidos. Por outro lado, surge pela LGPD uma responsabilidade das empresas no tocante à adequada avaliação das empresas com as quais as informações são compartilhadas, assim como o conteúdo a ser compartilhado. Processos internos que regulem o compartilhamento passam a ser essenciais, mas falta maturidade.
15 - Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	O incentivo à inovação é essencial para o desenvolvimento dos países e das organizações. A motivação e o incentivo à estas atividades se inserem naturalmente, quando devidamente compreendido, como possíveis subprodutos da LGPD, nesta nova era da economia digital global. Nesta área o único possível cuidado seria o de evitar que a transparência em toda sua extensão não venha a violar a necessária confidencialidade e proteção de dados pessoais, que cercam todos os processos de inovação. Observem nossas propostas incluídas nos Anexos.
PARA AS QUESTÕES INDICADAS, TEMOS NO ANEXO 1 DADOS COMPLEMENTARES COM FUNDAMENTAÇÃO E JUSTIFICATIVAS – Documento: Anexo1TSIOT.pdf	
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Dúvidas ou questionamentos – Contatar João Roberto Peres – jperes@komp.com.br

ANEXO 1 - CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1/2021

NOME DA INSTITUIÇÃO: Tudo-sobre-IoT – KOMP Security, Uberconsult e outras

Textos em azul escuro estão dispostos no documento PARA ENVIO DE CONTRIBUIÇÕES.

Usamos o acrônimo **EPPs** para designar todos os tipos de empresas de pequeno porte.

Tópico/Questão

1- Quais são os desafios/problemas regulatórios relacionados ao tema?

Os grandes Desafios que identificamos:

A. **Qualificação do porte das organizações brasileiras –** Acreditamos que a Lei complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte e complementos, devam ser consideras, no entanto "não" se fazem adequadas para o enquadramento de empresas quanto ao porte para atendimento aos ditames da Lei 13.709:2018, mesmo considerando o Artigo 55J –XVIII da Lei nº 13.853, de 8 de julho de 2019 que requer posicionamentos da ANPD, pois, o ***enquadramento deveria ser realizado, não só com base no faturamento anual, mas com base no volume, tipo de dados (regular, sensível, crianças e adolescentes) criticidade, local e frequência de tratamento de dados pessoais***, que uma empresa necessita para operar. Como reflexão, encontramos na prática, grandes organizações operando em B2B, tratando dados pessoais comerciais, de baixa criticidade, e em volumes menores, que muitas empresas de muito pequeno porte.

Fundamentação e justificativas:

Este grande desafiou já foi identificado pela ANPD e também endereça a questão 5 - Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte? – Aqui gostaríamos de observar que no Brasil em maio de 2020, segundo dados do portal "datasebrae", dados fornecidos pela Receita federal do Brasil, havia um total de 19.228.025 empresas de todos os portes e de todos os tipos de atividades (CNAE). Desse total, selecionamos no portal as empresas (CNPJs) classificadas como MEI, ME e EPP, de todos os tipos de CNAE, totalizando 17.293.316 – dados obtidos e confirmados em 25/02/2021 – disponíveis na URL https://datasebrae.com.br/totaldeempresas/.

Em nossa pesquisa, consideramos que MEIs (Microempreendedores Individuais) devem representar hoje, quase 50% dos CNPJ brasileiros. As EPPs e as MEs totalizam 7.482.833 empresas. As empresas médias e grandes totalizam apenas 1.934.709.

No portal do governo brasileiro https://www.gov.br/governodigital/pt-br/mapa-de-empresas em 25/02/2021 encontramos que o país possui 20,1 milhões de empresas, das quais 373 mil foram abertas em janeiro de 2021.

Mas qual é o significado desses dados, considerando nosso objetivo?

O alcance de qualquer medida regulatória da ANPD para flexibilização ou intensificação de requerimentos, para esse público, sempre será muito significativa para o país. Por outro lado, com base no artigo do "XXXII Encontro da ANPAD (Associação Nacional de Pós-Graduação e Pesquisa em Administração)" intitulado "Lei Geral da Micro e Pequena Empresa Versus Small Business Act: uma Comparação entre as Determinações para

Inserção das MPEs nas Compras Governamentais", de Autoria: Marina Figueiredo Moreira, José Matias-Pereira, temos como determinante na introdução do artigo as seguintes considerações:

"*As micro e pequenas empresas brasileiras – MPEs – são reconhecidas por sua representatividade econômica. Esse segmento responde por 99,2% de todos os empreendimentos brasileiros, sendo responsável pela geração da maioria dos postos de trabalho formais e pela totalidade dos informais (SEBRAE-SP, 2005). Apesar de sua grande força econômica, as micro e pequenas empresas brasileiras enfrentam grandes fragilidades, principalmente no tocante à capacidade de competir no mercado frente às demais empresas*. "

No resumo introdutório destaca-se "*A legislação brasileira (Lei 123/2006) apresenta em alguns momentos, determinações muito próximas às da correspondente legislação norte-americana, o que permite compará-las. Este artigo se propõe a estabelecer comparação entre essas duas legislações, revelando seus pontos comuns e suas diferenças e considerando, nos dois casos, o contexto de importância e inserção econômica das* ***micro e pequenas*** *empresas na economia de cada país*."

Na página 7 do artigo que trata da 'Lei Geral da Micro e Pequena Empresa X Small Business Act' - Encontramos: "*Após analisar a Lei Geral da Micro e Pequena Empresa e o Small Business Act, é possível estabelecer comparação entre suas determinações, objetivo inicial deste estudo. No entanto, para que a comparação seja válida e cumpra seu objetivo, é necessário considerar as diferenças econômicas entre os dois países. Cabe, portanto, comparar inicialmente o impacto exercido pelas micro e pequenas empresas nas economias brasileira e norte-americana*."

O quadro abaixo é muito elucidativo, para que possamos compreender e projetar em 2021 a importância e evolução desse comparativo.

	Brasil	Estados Unidos
Total de micro e pequenas empresas	Eram 4,9 milhões de micro e pequenas empresas em 2002.	Eram 22,9 milhões de pequenos negócios em 2002.
Participação nos postos de trabalho	Responsáveis por 60% dos empregos formais e a totalidade dos informais.	Responsáveis pela criação de 75% dos novos postos de trabalho.
Participação no PIB	São responsáveis por 20% do PIB brasileiro.	São responsáveis por 40% do PIB norte-americano.
Participação nas exportações	Detêm 2% das exportações brasileiras.	Constituem 97% dos exportadores norte-americanos.

Tabela 2: Micro e pequenas empresas nas economias brasileira e norte-americana.
Fonte: elaborado pelos autores a partir de informações de Sachs (2003) e SEBRAE-SP (2005).

Em nossa avaliação, a projeção de dados de 2003/2005 para os dias de hoje, coloca o Brasil muito próximo ao que se encontrava os Estados Unidos em 2002, ou seja, temos hoje próximo de 19 milhões de empresa que se qualificam MEI, ME e EPP (empresas de pequeno porte genericamente EPPs), responsáveis próximo de 70% dos empregos formais no país.

Obs.: considerando apenas a representatividade de dados pessoais, dos colaboradores com empregos formais das EPPs, temos uma quantidade muito significativa de dados pessoais (próximo de 55 milhões de pessoas), que a Lei 13.709:2018 deva impactar. Da mesma forma, seria bom observar que a correspondência brasileira quanto as exportações, tendem a se alinhar ao padrões norte-americanos, o que significa um grande transito de dados transnacionais entre organizações.
O relatório estava disponível em 25/02/2021 em:
http://www.anpad.org.br/admin/pdf/APS-B1341.pdf

Resumindo - Entendemos que este tema seja um grande desafiou, e uma oportunidade para a regulação inovadora da ANPD no mundo, onde "**critérios complementares como: Volume, Tipo de dados, Criticidade, Local e Frequência**", adicionados aos atuais utilizados normalmente para qualificar o porte das empresas (quantidade de colaboradores e faturamento anual), possam realmente contribuir para uma maior assertividade e justiça social. Maiores detalhes forneceremos na resposta da **quinta questão** formulada pela ANPD.

Pedimos atenção especial as empresas qualificadas como do terceiro setor - "Terceiro Setor é composto por organizações de natureza "privada" (sem o objetivo do lucro) dedicadas à consecução de objetivos sociais ou públicos, embora não seja integrante do governo (Administração Estatal)" – são as OS, ONG, as OSCIP e Institutos, etc. Muitas são EPPs de fato.

Podemos colaborar a posterior, assessorando a ANPD nesta questão, com maiores detalhes das nossas indicações. jperes@komp.com.br

B. **Considerar aspectos culturais, sociais e econômicos brasileiros –** Apesar de serem temas conhecidos, realçamos a necessidade de entender o Índice chave **IPCLBrasil** - (Índice de percepção do cumprimento de Leis no Brasil - (compliance with the law) - https://direitosp.fgv.br/publicacoes/ipcl-brasil), que necessitaria ser atualizado e focado agora para a LGPD em 2021.

Compreender a efetiva "resistência" dos empresários brasileiros e seus reais motivos, em não adotar os requerimentos legais da LGPD, passa a ser fundamental para o planejamento estratégico de ações que possam acelerar o convencimento e a adequação, sem criar os estigmas das sanções.

Nesta mesma linha, é importante compreender o problema da não adesão à LGPD, considerando a inércia similar ocorrida na União Europeia com a GDPR, no seu primeiro e segundo ano, após sua entrada em vigor em 25 de maior de 2018.

Fundamentação e justificativas:

Tradicionalmente é usual dizer no Brasil, que determinada Lei não pegou, ou seja, não foi aceita pela população, que não buscou conhecer o teor, muito menos em atender aos seus requerimentos. Até mesmo algumas legislações, muito objetivas e de fácil compreensão, como o caso da Lei 11.705:2008, conhecida como Lei Seca, com o intuito de reduzir acidentes de trânsito gerados por motoristas que estão sob efeito do álcool, sofreu rejeição e foi muito descumprida, necessitando endurecimento de ações de fiscalização, elevadas multas e penalização criminal.

O problema de atendimento a regramentos e Leis governamentais, no mundo todo, é

muito parecido, mas sempre influenciado por questões culturais e socioeconômicas de cada nação. No caso brasileiro da LGPD, as empresas, "Controladores", passaram a entender a Lei como um custo adicional desnecessário e com resultados inócuos para os Titulares, que desde sempre alegaram que não possuem nada para esconder, e fornecem os seus dados de forma aberta para tudo. Em nosso país a identificação dos riscos digitais pela maioria da população é quase zero. A palavra Privacidade é pouco compreendida em sua profundidade e alcance.

Quando olhamos os países da União Europeia sobre a mesma ótica, lá também houve resistência na adoção das determinações legais, mesmo já possuindo regramentos evolutivos no tema, há mais de 20 anos, antes da divulgação do (UE) 2016/679 GDPR que é o regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu, que entrou em vigor em 25 maio de 2018. Vamos aos fatos – encontramos manchetes e notícias com o seguinte teor:

"**Na Europa, menos de 30% das empresas estão adequadas à GDPR**" - 11 de outubro de 2019 -

(Mais de um ano após a vigência da GDPR da Europa, o Capgemini Research Institute constatou que as empresas não levaram a sério o novo regulamento. Apenas 28% atingiu a conformidade, o que contrasta uma pesquisa semelhante no ano passado — na ocasião, 78% diziam estar preparados quando o regulamento entrou em vigor em maio de 2018. No entanto, as organizações estão percebendo os benefícios de estar em conformidade: 81% dizem que a GDPR teve um impacto positivo em sua reputação e imagem de marca.)...

https://www.ecommercebrasil.com.br/noticias/na-europa-menos-de-30-das-empresas-estao-adequadas-a-gdpr

"Após 2 anos, 40% das empresas na Europa ainda não estão adaptadas a GDPR"

(Um estudo desenvolvido pela Check Point Software Technologies, empresa de cibersegurança, mostra que muitas empresas europeias ou que prestam serviços no Velho Continente ainda não estão totalmente em conformidade com a GDPR (Regulamentação Geral de Proteção de Dados da União Europeia). De acordo com o levantamento, 40% das companhias estão parcialmente em compliance com a norma ou estão apenas no início da adaptação da GDPR.

O mesmo estudo apontou alguns dos investimentos feitos pelas empresas europeias para a adaptação a LGPD. Eis o que as empresas informaram:

- *Adoção padrão de **medidas de segurança** (44%);*
- *Promoção de **ações de formação para funcionários**, para aumentar o seu conhecimento dos riscos de segurança de dados (41%) e;*
- *Implementação de um sistema de **controle de acessos e de encriptação** (41%).*

Investimentos (em valores)

*O investimento das empresas no compliance da GDPR foi outro ponto de destaque do levantamento. Houve um aumento de investimentos: 27% dos entrevistados investiram entre **US$55 mil a US$165,3 mil**, os quais apresentaram um retorno (ROI) em forma de benefícios como aumento da confiança do consumidor e em uma maior segurança dos dados.)...*

https://www.oconsumerista.com.br/2019/12/dois-empresas-europa-gdpr/

Conclusão

Como se pode observar, este desafio da ANPD, em superar as questões "culturais e socioeconômicas" que influenciam o acatamento da LGPD, é complexo e requer um trabalho de base de conscientização, para divulgar os objetivos e as vantagens que a Lei traz para os cidadãos e para o país. Da mesma forma, as pequenas empresas, terão de buscar soluções criativas e econômicas para viabilizar a capacitação dos colaboradores e ampliar a curva das medidas de segurança que devem ser adotadas. Entendemos que a conscientização e capacitação possam ser evolutivamente fomentadas em cursos gratuitos já disponíveis na web, parcerias da ANPD com portais comerciais EAD e oferta de cursos gratuitos nos temas de maior impacto para as organizações de pequeno porte.

Quanto as ferramentas de segurança para EPPs, acreditamos que o mercado mundial já disponha de softwares Livres, de código aberto, de alta reputação para soluções de Anonimização, Criptografia forte FIPS-140-2, Sistemas Firewall, Sistemas Antivírus, IDS/IPS, entre outros, bem como software freewares, que devidamente selecionados possam ser um bom referencial para superar as questões econômicas dessas empresas de pequeno porte, de fato.

Podemos colaborar a posterior, assessorando a ANPD nesta questão, com maiores detalhes das nossas indicações. jperes@komp.com.br

C. **Práticas metodológicas e normativas em uso cotidiano nas empresas nacionais** – Entendemos que infelizmente no nosso país a adoção às Normas Internacionais (ISO) e melhores práticas possui baixa aderência – No campo e na prática, observamos que padrões fundamentais como a Norma NBR ISO/IEC 27002 (código de práticas e controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação), traduzida e publicada como NBR ISO 17799:2000, e atualizada oficialmente para ABNT NBR ISO/IEC 27002 em julho 2007, até hoje é muito pouco conhecida e praticada nas nossas empresas de todos os portes por não saberem calcular o ROSI (Return on Security Investment). Aqui o grande desafio é compreender e planejar ações motivacionais que possam sensibilizar empresários na busca de incrementar padrões e melhores práticas, mínimas necessárias para a competitividade, das nossas empresas, e para o crucial atendimento a Privacidade e Proteção de Dados.

Fundamentação e justificativas:

2021 – Vivemos em mundo de padrões estabelecidos – para a maioria das áreas de conhecimento aplicável em organizações empresarias, encontramos melhores práticas amplamente divulgadas, estabelecidas em instrumentos normativos, guias e frameworks, muitos disponíveis gratuitamente e outros sendo utilizados como base para a certificação de conhecimentos profissionais.

Estamos nos referindo a grandes e tradicionais marcos como os padrões:

- ITIL (Information Technology Infrasructure Library) que se tornou a ISO/IEC 20000:2005, que é um conjunto de regras que define as boas práticas de gestão de serviços de TI;
- PMBOK (Project Management Body of Knowledge), que é o tradicional conjunto de práticas na gestão de projetos organizado pelo instituto PMI (Project Management Institute);
- CobiT (Control Objectives for Information and Related Technologies), que é um framework evolutivo de boas práticas de segurança, gestão e governança de TIC, criado pela ISACA (Information Systems Audit and Control Association) há 25 anos atrás.

Existem algumas dezenas de padrões altamente recomendáveis, para a evolução da maturidade operacional das organizações empresariais.

Considerando as necessidades endereçadas para o atendimento a LGPD, na sua fase de planejamentos e efetiva implementação, ao desenvolvermos na KOMP Security Brasil o nosso framework de solução para o mercado, que nominamos "PrivacidadeOK", identificamos a necessidade de aplicar as melhores práticas como base minimamente, atendendo os seguintes padrões:

- **PMBOK** – entendemos que a implementação da LGPD, em qualquer empresa, deva ser conduzida como um Programa composto por Projetos sequenciais e interdependentes, com escopo, prazo e custos completamente definidos e gerenciados. Isso devido a aplicação de recursos humanos com conhecimentos multidisciplinares, assim como estruturas metodológicas e ferramental de softwares apropriados.
- **BABOK** - Business Analysis Body of Knowledge – é necessário conhecer o negócio do cliente. Para cada tipo e arquitetura de negócio existem especificidades a serem consideradas nos processos de tratamento de dados pessoais.
- **TOGAF** - The Open Group Architecture Framework, estabelece uma arquitetura corporativa com quatro níveis ou domínios: Negócios, Aplicação, Dados e Tecnologia. Esse instrumento permite obter uma visão ampla do inter-relacionamento e interdependências nas estruturas empresariais, para a melhor compreensão do uso de dados pessoais nas organizações.
- **CBOK-BPM** – Common Body of Knowledge - Business Process Management ou Gerenciamento e Mapeamento de Processos do Negócio. Fornece as bases para o mapeamento estruturado de processos, bem como, sua documentação e evolução para a automação da gestão.
- **DMBOK** (DAMA-DMBOK) Data Management Body of Knowledge – framework completo para a Gestão e Governança de Dados. Este padrão é fundamental para que uma organização possa estabelecer um "programa de governança de dados" que realmente alcance êxito. Utilizamos as bases do padrão, para realizar mapeamento de dados e estabelecer a documentação de Metadados das empresas.
- **Norma ISO 20000** – Trata da gestão da Qualidade de Serviços de TIC e outros. Fundamental para entender e ajustar questões operacionais, manter o registro de operações, estabelecer o registro e as evidências de incidentes operacionais e de segurança, entre outros aspectos de gestão de tecnologias e infraestrutura.
- **Norma ISO série 31000** – Avaliação e Gestão de Riscos - Fundamental para avaliar riscos de não conformidade corporativa – pode ser adicionada com o padrão normativo da ISO/IEC 27005, que trata da gestão de riscos de segurança da informação.

- **Normas ISO/IEC série 27000** – 27002 (melhores práticas de Segurança da Informação), 27001 (sistema de Gestão da Segurança da Informação) – 27701 (complemento da 27001 com foco em sistema de Gestão PII - especifica os requisitos e fornece diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de gestão de Privacidade da Informação (SGPI)...
- **SABSA** - Enterprise Security Architecture – metodologia avançada de segurança focada nas informações e nos negócios. Pode ser aplicada com um processo de gestão da segurança empresarial em todos os aspectos, de forma matricial e simplificada nas empresas.
- **PbD** (Privacy by Design-RYERSON methodology) composto por 07 Princípios, 30 critérios e 95 controles, para alcançar de forma "certificável" o Privacy by Design e Privacy by Default, requeridos na GDPR/LGPD. A aplicação real desse padrão é fundamental para garantir o crescimento incremental da cultura de Privacidade e ações efetivas de Proteção de Dados Pessoais, em todos os processos operacionais das empresas.
- **SCF** - Secure Controls Framework - é um catálogo de controles que trata de Privacidade e Segurança de forma abrangente, com controles projetado para permitir que as empresas projetem, construam e mantenham processos, sistemas e aplicativos seguros, em especial para proteger e atender incidentes de segurança de dados e ataques cibernéticos.
- **Norma ISO 38500** – Trata da Governança de TIC – importante conhecer e observar sua aplicação ou recomendar a adoção dos seus 6 princípios.
- **Norma ISO 19600** – Trata da Gestão de "Compliance" nas organizações. O padrão de gestão deve ser aplicado, mesmo que inicialmente só sobre a LGPD.
- **Padrões metodológicos** estabelecidos pela EU para atender a GDPR, considerando estarem alinhados aos requerimentos da LGPD:
    - 1 - PIA (Privacy Impact Assessmente Methodology)
    - 2 - LIA (legitimate Interests Assessment Methodology)
    - 3 - DPIA (Data Protection Impact Assessment Methodology)
    - 4 - RoPA (Record of Processing Activities Methodology)
- Diversa outras referências de fundamentação.

Como se pode observar, nosso entendimento é que na implementação de soluções para que uma empresa possa atender aos requerimentos da LGPD, de forma estruturada e completa, se faz necessário que estas possam compreender e aplicar determinados padrões internacionais de melhores práticas, minimamente como os que adotamos em nosso framework "PrivacidadeOK". No entanto, a realidade de mais de 90% das empresas brasileiras é não possuir ou adotar padrão algum, normalmente operam sem formalismos ou práticas regulares, o que denota um nível de maturidade organizacional muito baixo.

Conclusão

Entendemos que o grande desafio da ANPD neste caso, é compreender a questão e fomentar através de campanhas de esclarecimento, a necessidade das organizações de todos os tipos e portes em adotar gradativamente as melhores práticas internacionais. Da mesma forma, compreender que é quase impossível exigir que empresas de pequeno porte de fato, possam implementar os requerimentos de tratamento de dados da LGPD, em seus processos

operacionais, de forma consistente e concreta, considerando praticamente a inexistência de adoção de melhores práticas, em todas a áreas de conhecimento organizacional necessárias.

Podemos colaborar a posterior, assessorando a ANPD nesta questão, com maiores detalhes das nossas indicações. jperes@komp.com.br

D. **Estabelecer Níveis de Maturidade a serem alcançados** – Entendemos ser fundamental estudar e estabelecer patamares a serem alcançados, tanto na adequação à LGPD, Governança de Dados e Cultura de Privacidade e Proteção de Dados e a evolução dos conhecimentos dos Encarregados em um horizonte de tempo pré-definido. Aqui recomendamos uma adaptação dos modelos internacionais CMMi (Capability Maturity Model Integration) e PCMM (People Capability Maturity Model). -- Vide fundamentação e justificativas no "Anexo 1".

Fundamentação e justificativas:

Como já identificamos um dos grandes desafios da ANPD está ligado as práticas metodológicas em uso nas empresas brasileira, da mesma forma, outro desafiou em paralelo será estabelecer **níveis de maturidade** para os **processos operacionais da LGPD** nas empresas de todos os portes. Para compreensão é importante exemplificar, como compreendemos (KOMP) e aplicamos as questões de porte organizacional quando ofertamos soluções de adequação da LGPD para o mercado:

Definição de porte e maturidade organizacional – para que as empresas entendam.
Dependência de tratamento de dados pessoais – exemplos:

ADEQUAÇÃO LGPD FACILITADA – Nível de Maturidade médio – Perfil Organizacional:

- Empresa grande/muito grande, pública ou privada
- Banco de Dados diversos; >1.000.000 de registros correlacionados de dados pessoais
- Forte fundamentação Legal e aderência a princípios de tratamento de dados
- Forte uso de melhores práticas internacionais ITIL, CobiT, ISO...
- Infraestrutura de TIC e operacional Governada Corporativamente
- Áreas de Segurança da Informação e Compliance muito ativas
- Bases de Dados Estruturadas e com boa Governança de dados
- Dicionário de Dados estabelecido e atualizado (estrutura de metadados documentada)

ADEQUAÇÃO LGPD TRABALHOSA – Nível de Maturidade baixo

- Empresa Média a Grande, pública ou privada
- Até 500.000 registros correlacionados de dados pessoais por BD
- Boa base de fundamentação Legal e princípios de tratamento
- Baixo uso de melhores práticas internacionais
- Infraestrutura de TIC e operacional com melhores práticas ITIL/CobiT
- Áreas de Segurança da Informações e Compliance estabelecidas
- Bases de Dados Estruturadas em sistemas integrados, sem governança
- Dicionário de Dados em desenvolvimento (estrutura de metadados)

ADEQUAÇÃO LGPD COMPLEXA – Nível de Maturidade ZERO

- Empresa pequenas e médias pública ou privada
- Até 50.000 registros correlacionados de dados pessoais
- Média fundamentação Legal e aderência a princípios de tratamento
- Melhores práticas internacionais ITIL, CobiT, ISO,... ***inexistentes***
- Infraestrutura de TIC e operacional com baixa maturidade
- Áreas de Segurança da Informações e Compliance ***inexistentes***
- Bases de Dados esparsas e ou desestruturadas
- Sem documentação das estruturas de dados

A nossa visão é que a complexidade de implementar soluções da LGPD é inversamente proporcional a cultura organizacional, recursos humanos, uso de melhores práticas e infraestrutura das organizações. É obvio que quanto mais organizada e estruturada uma empresa seja, isto é, quanto maior o nível de maturidade organizacional, a implementação da LGPD fica facilitada. Isso significa dizer que o trabalho de Consultoria, jurídica, técnica e de aculturamento em pequenas organizações, sobre Privacidade e Proteção de Dados, TIC, entre outros aspectos, é muito maior e demanda mais tempo, e custos na prática.

Como proposta entendemos ser necessário o estabelecimento de níveis de maturidade pela ANPD para que o mercado compreenda a necessidade de evolução contínua, e para isso convêm observar dois olhares, ou seja; visualizar a **maturidade dos processos organizacionais** das empresas e em paralelo visualizar a **maturidade profissional** de seus colaboradores, em especial dos encarregados DPOs.

Como padrão clássico de "modelo de maturidade" recomendamos "**para a LGPD à adaptação do padrão CMMi**" (Capability Maturity Model Integration) – foco em "Integrated Product and Process Development" (IPPD - Desenvolvimento Integrado de Processo e Produto), desenvolvido originalmente pelo SEI (Software Engineering Institute) da Universidade Carnegie Mellon, hoje de propriedade e gerenciamento pelo **Instituto CMMI**, uma organização da ISACA.

https://www.businesswire.com/news/home/20160303006773/pt/

http://www.isdbrasil.com.br/artigos/cmmi2.0.php

Veja um exemplo de integração/adaptação –"DATA MANAGEMENT MATURITY (DMM)SM MODEL": baixe o guia - https://cmmiinstitute.com/getattachment/cb35800b-720f-4afe-93bf-86ccefb1fb17/attachment.aspx disponível em 25/02/2021.

Quando falamos de "Modelo de Maturidade para a LGPD", estamos visualizando ações já em prática, em especial para a GDPR, como o proposto pela IAPP no documento "The GDPR Maturity Framework" que pode ser baixado através do link, disponível em 25/02/2021 - https://iapp.org/media/pdf/resource_center/PrivacyCulture_GDPR_Maturity_Framework.pdf

No caso de modelo de maturidade, em questões de "Privacidade", indicamos os Modelos da FORTPRIVACY, e da IAPP, que podem ser baixados com os links - disponíveis em 25/02/2021:

https://www.fortprivacy.ie/media/1053/introducing-the-fort-privacy-maturity-model.pdf

https://iapp.org/resources/article/2012-06-01-aicpa-cica-privacy-maturity-model/

Para a aplicação nas questões de maturidade profissional, ainda indicamos como complemento o modelo de gestão "People Capability Maturity Model (P-CMM)" que é uma Avaliação sobre o

Nível de Maturidade em Gestão de Pessoas e os Programas de Treinamento, Desenvolvimento e Educação Corporativa. Tanto o CMMi e o P-CMM possuem a mesma origem de concepção, mas utilizam estruturas diferenciadas para alcançar seus objetivos específicos.

Veja referências e estudos importantes sobre o tema:
http://www.anpad.org.br/diversos/down_zips/63/2012_GPR604.pdf
https://www.scielo.br/pdf/rac/v13n2/05.pdf
https://cio-wiki.org/wiki/People_Capability_Maturity_Model_(P-CMM)
https://home.kpmg/in/en/home/services/advisory/management-consulting/business-excellence/spi-pcmm.html

Conclusão
Acreditamos que a ANPD deva estabelecer em seu portal web, referências de níveis de maturidade organizacional, especificando o que julga necessário as empresas alcançarem para se qualificar em determinado nível. A divulgação dessa visão e de requerimentos por nível, poderá incentivar um processo de comparação (Benchmarking) no meio empresarial, e na evolução dos quadros de colaboradores das organizações.

Nós (KOMP) já aplicamos uma adaptação de modelo de maturidade para que nossos clientes entendam minimamente as nossas ofertas de soluções e a qual nível eles podem alcançar.

E. **Planejamento Estratégico de Programas de Motivação e Alcance** – Entendemos que se faz necessário priorizar o planejamento de inciativas como; equacionar campanhas públicas para "Agentes de Tratamento de Dados" em seu apoio, algumas que sugerimos aqui e as detalhamos no Anexo correspondente – por exemplo:

a) Campanha de divulgação "**Só não cumpre a LGPD quem não quer**" – para atender as empresas qualificadas como EPP (empresas de Pequeno Porte para a LGPD). No Portal da ANPD poderia haver um "Guia de Melhores Práticas" para esse perfil de empresa, como a Autoridade

de Proteção de Dados Inglesa "ICO. (Information Commissioner's Office)" divulga em sua página web "Data protection advice for small organisations". https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/

b) Outra hipótese seria uma campanha ofertando um SELO ANPD "**Empresa Colaboradora ANPD – fomentando a Cultura da Privacidade e Proteção de Dados**", para as empresas que investirem ou cooperarem em ações de aculturamento de outras organizações menores, que se inscrevam graciosamente em seus Portais de Conhecimento EAD.

c) Como terceira hipótese, a produção da campanha e SELO ANPD "**Empresa Aderente a LGPD - Self Certified**", pode ser muito motivador - recomendamos estabelecer parâmetros de requerimentos objetivos e práticos que possam ser auditáveis, e serem efetivamente alcançados pelas empresas.

> Para atender o proposto nesta terceira hipótese **c)**, entendemos que algumas práticas normatizadas em outras áreas, como é o caso do padrão estabelecido pelas Normas de "Autodeclaração de Conformidade", tratada nas normas internacionais ISO/IEC 17050:2004-1 e ISO/IEC 17050:2004-2. A parte 1 da 17050 foi desenvolvida com o objetivo de fornecer requisitos gerais para a Declaração de Conformidade do Fornecedor (SDoC, na sigla em inglês), possam servir de embasamento no caso da LGPD.
>
> Sabemos que o tema "Certificação" é polêmico e conhecemos as implicações e todas as questões de "Acreditação Oficial", através de delegações do INMETRO e alinhamentos internacionais, no entanto, avaliações de terceira parte estão ganhando força no mundo contemporâneo e passaram a ser um instrumento de incentivo a conformidade e gerador de novos empregos. – vide: http://inmetro.gov.br/Credenciamento/index.asp

Fundamentação e justificativas:

Entendemos que a ANPD deva desenvolver um processo interno de Planejamento Estratégico de longo alcance, para atender as especificidades das empresas classificadas como EPPs, que permita estrelecer um ranking de prioridades, de forma que se fundamente uma estrutura para alcançar o apoio e patrocínio direto e indireto da sociedade brasileira, nos meios acadêmicos e empresariais.

A nossa proposta **a)** Campanha de divulgação "**Só não cumpre a LGPD quem não quer**", tem como base a visão didática de nosso framework de solução para adequação da LGPD, para pequenas organizações, denominado "PrivacidadeOK", que é fundamentado em instrumentos de capacitação na modalidade "**faça você mesmo**", orientando o passo a passo, para alcançar os resultados definidos e esperados continuamente. Ofertamos aos clientes vídeo-aulas suportadas on-line por "coaching", através de Consultores experientes, um grande número de guias de orientação, dezenas de templates e sugestões de ajustes conforme a atividade core da empresa, indicamos ferramenta de softwares livres ou freeware para todo o necessário na LGPD, ensinamos a instalar e usar, entre outras estratégias que permitem expressiva redução de custos as pequenas organizações.
Por nossa experiência, acreditamos que seria possível contribuir com a ANPD, na formatação de uma modalidade de modelo padronizado (framework), que possa ser replicado por outras empresas interessadas em apoiar esse enorme mercado das EPPs carentes. Os valores cobrados poderiam ser sugeridos ou propostos limites de preço e parcelamentos, que sejam razoáveis.

Entendemos sim que "**Só não cumpre a LGPD quem não quer**".

A proposta **b)** "**Empresa Colaboradora ANPD**", pode ser ampla, com base em diversas campanhas de captação de patrocínio e apoio de médias e grandes empresas, ou mesmo delegada a uma "**ong.**" que possa se dedicar as questões sociais da Privacidade e Proteção de Dados Pessoais, aos moldes que fez, como exemplo; o "Instituto Ethos" que atua em quatro grandes áreas: Direitos Humanos, Gestão para o Desenvolvimento Sustentável, Integridade e Meio Ambiente, congregando apoios das maiores empresas do país.

No caso da proposta **c) "Empresa Aderente a LGPD - Self Certified"** – é onde detemos maior conhecimento para materializar e apoiar a ANPD, mas entendemos a complexidade regulamentar, estratégica e política do tema. No entanto, acreditamos na **inovação e flexibilização** necessária aos moldes norte americano, onde as "Avaliações de Terceira Parte" operam como os serviços de "Peritos Credenciados", para atender o Ministério Público em processos judiciais, inclusive no Brasil. Esse modelo poderia ser aplicado para **validar** a "Auto-declaração de Conformidade a LGPD".

Uma recomendação da ANPD, para as EPPs poderia ser: "Uma organização externa colaboração na implementação de adequação, enquanto outra, totalmente distinta, valida a devida efetividade do implementado". Essa indicação com o tempo, poderia passar a ser exigência.

Conclusão

Temos diversas outras propostas, mas iriamos nos estender demais, no entanto, essa nossa proposta final é chave para o futuro brasileiro e para a sustentação da aplicabilidade da própria legislação:

- **Parceria com o MEC** – A ANPD poderia propor ao MEC incluir na "Base Nacional Comum Curricular", no currículo de "Tecnologia e Computação", desde da educação Básica infantil e fundamental, ensino médio e profissional Técnica, no eixo **Cultura Digital**, os temas "Privacidade e Proteção de Dados" **em sua profundidade**.

Para compreensão indicamos os links:

http://basenacionalcomum.mec.gov.br/implementacao/praticas/caderno-de-praticas/aprofundamentos/193-tecnologias-digitais-da-informacao-e-comunicacao-no-contexto-escolar-possibilidades

https://curriculo.cieb.net.br/

Esta contribuição básica, foi produzida com o incentivo da **Comunidade Tudo-sobre-IoT** que pode ser acessada no Portal - https://tudosobreiot.com.br/

Participaram das pesquisas e colaboração:

Coordenação: João Roberto Peres – Komp Security Brasil - https://www.komp.com.br/

jperes@komp.com.br

Integrantes: Janne Kaunert - Kaunert Direito Digital - https://digitalk.adv.br/

João Adolfo de Resende Ponchio – Uberconsult - https://uberconsult.com.br/

Josmar Giovannini - Conformidados - https://www.conformidados.com.br/

Marcela Arruda – Rubes Naves Santos Jr Advogados - http://www.rnsj.com.br/

Orlando Arnaud – Uberconsult - https://uberconsult.com.br/

Thelma Troise – Tudo-sobre-IoT - https://tudosobreiot.com.br/

Wagner Pozzer - Rubes Naves Santos Jr Advogados - http://www.rnsj.com.br/

Dados sobre: informações questionadas a respeito da segurança de devices IoT em computação de borda (**edge computing**) ou (fog computing) pelo **Sr. Fabricio Guimarães Madruga Lopes** - Coordenador de Normatização.

O mercado nacional já dispões de ações de capacitação e preocupação com o tema ofertando cursos de IoT, por exemplo, nas seguintes entidades:

Pelo portal "**Tudo sobre IoT**" - https://tudosobreiot.com.br/

Fórum Brasileiro de IoT – no Portal **Cyber Security Group** - https://csgiot.org/, do qual o Sr. João Peres, também é responsável.

Na organização **FUSE-IOT – Academy**, com cursos previstos e em andamento in-company - https://academy.fuseiot.io/

Podemos fornecer maiores detalhes.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Associação Brasileira de Franchising ("ABF"), associação civil sem fins lucrativos, inscrita no CNPJ/MF sob o n.º 57.806.978/0001-62, com domicílio na cidade de São Paulo, Estado de São Paulo, na Av. das Nações Unidas, n.º 10.989, 11ºandar, conj.112, CEP 04578-000.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quais são os desafios/problemas regulatórios relacionados ao tema?	**1. Obrigações complexas e onerosas.** Microempresas ("**Micro**"), empresas de pequeno porte ("**EPP**") e o microempreendedor individual ("**MEI**"), conforme classificação dada pela LC 123 de 14.12.2006, possuem operações simplificadas, em regra, um ou mais computadores, com ou sem uso de rede para configuração de máquinas, os dados pessoais coletados decorrem, basicamente, da contratação de empregados, emissão de notas fiscais, prestação do serviço ao consumidor/cliente/paciente e/ou entrega do produto ao consumidor, o uso e a análise são limitados à prestação do serviço e/ou entrega do produto. O uso dos dados se esgota no momento da prestação do serviço e/ou entrega do produto. Os dados pessoais não são explorados ou comercializados sob nenhuma hipótese, portanto, o cumprimento de algumas das regras da Lei n.º 13.709/2018 são extremamente onerosas aos pequenos negócios. Os desafios são (i) cumprimento de obrigações complexas no que se refere ao tratamento de dados, assim entendidas, o mapeamento de riscos, o rastreamento de acesso e uso, o monitoramento desde a captura até a indisponibilidade, a gestão/avaliação de riscos contínua, prazos curtos para atendimento a direitos dos titulares; (ii) relatório de impacto à proteção de dados pessoais; (iii) nomeação de encarregado; e (iv) penalidades. **2. Nomeação de encarregado comum no Sistema de Franquia, regulado pela Lei n.º13.966/2019, sem caracterização de grupo econômico entre franqueadora e seus franqueados**. O sistema de franquia se caracteriza pela titularização pela franqueadora de uma marca, *know how*, sistema de distribuição ou outra forma de administração e gestão de negócio que pode ser cedido a um outro empreendedor para exploração independente, são empresas que se tornam

	associadas contratualmente, sem vinculação societária ou de interdependência, as empresas apenas exploram um negócio em comum. No sistema de franquia, podem existir ou não Micro, EPP e MEI associadas à franqueadora. Neste sistema, a franqueadora pode assumir obrigações de analisar os dados pessoais colhidos pelos franqueados, para auxiliá-los no desenvolvimento do seu negócio, assim como, a franqueadora poderá ceder dados para que o franqueado explore o seu negócio. Em razão da sua condição de controladora do dado, a franqueadora poderá nomear um encarregado para a rede, com ou sem compartilhamento de custos com os franqueados. O fato da nomeação de um encarregado de dados comum não pode significar a ocorrência de grupo econômico, sociedade empresarial, *joint venture* ou qualquer outro tipo de associação ou forma de ingerência no negócio do franqueado que descaracterize a relação empresarial nos termos da Lei n.º 13.966/2019. Deverá haver expressa disposição em regulamentação especial sobre tal condição. **2.1. Dados pessoais não compartilhados no Sistema de Franquia**. Por ser um sistema composto por empresas independentes, alguns dados pessoais não serão compartilhados, por exemplo, os dados de contratação dos empregados contratados pela franqueadora e pelo franqueado. Neste caso, se alguma violação ocorrer, ainda diante da nomeação do mesmo encarregado, a responsabilidade deverá recair sobre aquele que deu causa à violação, mantendo indene a outra parte, ainda que haja sido nomeado o mesmo encarregado de dados.
Existem sugestões para endereçamento do problema?	Sim, uma regulamentação especial que trate das obrigações mais flexíveis para Micro, EPP, MEI e para o sistema de franquia resolverão os problemas apresentados, por isso estamos sugerindo o modelo de regulamentação simplificada anexo.

Quais são as oportunidades relacionadas ao tema?	As oportunidades se referem à regulamentação específica dos temas e à aculturação/educação das partes interessadas. Sugerimos que a ANPD crie canais educativos para elucidação das questões, por exemplo, realizar seminários com magistrados e procuradores que poderão estar sujeitos ao enfrentamento destas questões. Divulgação para a imprensa destas nuances a respeito do cumprimento da lei. Celebração de convênios com entidades de classe para estudo e acompanhamento das questões, com divulgação de material elucidativo, nos termos do art. 55-J, XVIII da LGPD.

Quais são as experiências internacionais sobre o tema?	**<u>União Europeia (UE)</u>**: A GDPR (General Data Protection Regulation), Regulamento UE 2016/67 27.4.2016, nos termos do art. 30(5), dispensa o cumprimento da obrigaçã registro das atividades de tratamento de dados para as empresas qu possuem menos de 250 empregados; (ii) não ofereçam risco aos direit liberdades do titular; (iii) façam uso ocasional dos dados; (iv) não traten dados relativos à origem racial ou étnica, às opiniões políticas, às convic religiosas ou filosóficas, ou à filiação sindical, bem como o tratamento de da genéticos, dados biométricos para identificar uma pessoa de forma inequív dados relativos à saúde ou dados relativos à vida sexual ou orientação se de uma pessoa; e (v) não tratem os dados de condenações penais infrações. *"5. As obrigações a que se referem os n. 1 e 2 não se aplicam às empresas ou organizações com n de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco pa direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de d a que se refere o artigo 9., n. 1, ou dados pessoais relativos a condenações penais e infrações re no artigo 10.."* A GDPR recomenda que as autoridades nacionais dos países membros UE criem códigos de conduta para micro, pequenas e médias empre conforme art.40(1) e estipulem condições consideradas como de necessid específicas, de acordo com o art. 42(1). No entanto, a GDPR obriga as empresas que tiverem menos de empregados a cumprirem a obrigação de registro de tratamento de dado estas empresas (i) explorarem dados de maneira não ocasional; (ii) tratarem de dados específicos, considerados como sensíveis na legislação brasileira, art.9(1); e (iii) tratarem de dados relativos à condenação penal e infrações, art. 10. No âmbito da UE a **<u>interpretação é finalística</u>**, ou seja, ainda que a empresa seja considerada como micro, pequena ou média e explorar dados como sua atividade de negócio, a empresa estará sujeita ao cumprimento integral da GDPR, em especial, às obrigações de registro de tratamento de dados. Esta interpretação finalística sobre a forma como os dados são utilizados é absolutamente importante para a ANPD e para a regulamentação específica. Para o assunto "relatório de impacto à proteção de dados pessoais", a GDPR, no "considerando 91", trata das hipóteses em que ele é obrigatório: Deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais em âmbito regional, nacional ou supranacional, que possam afetar um número

Comentado [1]: No mesmo sentido, o "Considerando 13":
A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controle coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros. O bom funcionamento do mercado interno impõe que a livre circulação de dados pessoais na União não pode ser restringida ou proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controle, são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento. A noção de micro, pequenas e médias empresas ter em conta deverá inspirar-se do artigo 2.o do anexo da Recomendação 2003/361/CE da Comissão (5).

	considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos. Dever-se-á realizar também uma avaliação de impacto sobre a proteção de dados nos casos em que os dados pessoais são tratados para tomar decisões relativas a determinadas pessoas singulares na sequência de qualquer avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas. É igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controle de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrônicos, ou para quaisquer outras operações quando a autoridade de controle competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala. O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória. Sobre o assunto "designação do encarregado", o GDPR dispõe em seu a 37: item 1: O responsável pelo tratamento e o subcontratante designam encarregado da proteção de dados sempre que: a) O tratamento for efetu por uma autoridade ou um organismo público, excetuando os tribunais exercício da sua função jurisdicional; b) As atividades principais do respons pelo tratamento ou do subcontratante consistam em operações de tratam que, devido à sua natureza, âmbito e/ou finalidade, exijam um controle reg e sistemático dos titulares dos dados em grande escala; ou c) As atividad principais do responsável pelo tratamento ou do subcontratante consistam operações de tratamento em grande escala de categorias especiais de da nos termos do artigo 9 e de dados pessoais relacionados com condenaç penais e infrações a que se refere o artigo 10. item 2: Um grupo empresarial pode também designar um único encarreg da proteção de dados desde que haja um encarregado da proteção de da que seja facilmente acessível a partir de cada estabelecimento.

Comentado [2]: Ou seja, a realização de uma Avaliação de Impacto na Proteção de Dados (DPIA) é obrigatória sempre que o processamento pretendido represente um alto risco para os direitos e liberdades dos indivíduos, por exemplo, quando novas tecnologias são utilizadas.

Caracteriza-se alto risco quando:

- mecanismos automatizados de processamento e profiling são usados para avaliar indivíduos

- uma área de acesso público é monitorada em larga escala (por exemplo, CCTV)

- categorias especiais de dados ou dados pessoais relativos a condenações penais e infrações são processados em larga escala (por exemplo, dados de saúde)

Nota: As autoridades de proteção de dados também podem considerar outras categorias de processamento de dados como de alto risco.

Se as medidas indicadas na DPIA não eliminarem todos os altos riscos identificados, a Autoridade de Proteção de Dados deve ser consultada antes que o processamento de dados previsto ocorra.

Esta informação pode ser evidenciada no link: https://eur-lex.europa.eu/eli/reg/2016/679/oj

**

Lei de Proteção de Dados Australiana:

Privacy Act 1988 dispensa do cumprimento das obrigações os pequenos negócios (*small business*) que possuem volume de negócios anual (*annual turnover*) igual ou inferior a $3 milhões de dólares australianos, no conceito de volume de negócios consideram todas as fontes de receita, exceto ativos registrados, ganhos de capital, receitas decorrentes de transações de capital.

A lei australiana, no entanto, obriga o cumprimento por pequenos negócios que desenvolvem atividades em alguns ramos empresariais, tais como (i) serviços de saúde; (ii) exploração econômica de dados pessoais; (iii) presta serviço âmbito da Commonwealth; (iii)sociedades imobiliárias que utilizam dados locatários; (iv) empresas que fornecem informações sobre crédito (anális riscos de crédito); (v) entidade obrigada a reportar informações para os fin lei contra a lavagem de dinheiro e terrorismo; (vi) sindicatos e associaçã empregados; (vii) empresas de prestação de serviços de proteção de céd de votação, entre outras exceções definidas por regulamentação específi

Para os pequenos negócios obrigados ao cumprimento da Privacy Act 1 foram criados os Australian Privacy Principles (APP's) que se referem a regulamentação específica para estes pequenos negócios, para que dificulte ou onere a operação da atividade empresarial.

São 13 princípios a serem seguidos pelos pequenos negócios (i) transparê na gestão de informações pessoais (*open and transparent manageme personal information*); (ii) anonimato e pseudoanonimato (anonymity pseudonymity); (iii) captura de dados pessoais necessários e razoáv preferencialmente, não coletar dados sensíveis (*collection of solicited pers information*); (iv) gestão de dados não solicitados (*dealing with unsoli personal information*); (v) informar/notificar o titular sobre a captura de da pessoais (*notification of the collection of personal information*); (vi) infor sobre o uso e divulgação do dado pessoal (*use or disclosure of personal information*); (vii) preferencialmente não usar o dado para marketing direto (*direct marketing*); (viii) garantia de direitos na transferência internacional de dados (*cross-border disclosure of personal information);* (ix) não utilização de identificadores públicos *(adoption, use or disclosure of government related identifiers*); (x) qualidade do dado pessoal (quality of personal information); (xi) segurança do dado pessoal (security of personal information); (xii) acesso ao

Comentado [3]: Em interpretação à lei australiana, o site oficial do governo explica que não se enquadra como small business: "a business that sells or purchases personal information"; acho a tradução literal mais clara para esse propósito: "uma empresa que vende ou compra informações pessoais".

Ou ainda, a tradução literal do Privacy Act 1988 https://www.legislation.gov.au/Details/C2021C00024, diz: "Não é considerado pequeno negócio quem revele informações pessoais sobre outro indivíduo a qualquer outra pessoa para um benefício, serviço ou vantagem; ou ainda, quem fornece um benefício, serviço ou vantagem para coletar informações pessoais sobre outro indivíduo de qualquer outra pessoa".

https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/ Explicação que eles dão no site didático: "Um benefício, serviço ou vantagem pode ser qualquer tipo de pagamento financeiro, concessão, subsídio ou alguma outra vantagem ou serviço. Por exemplo, quando uma pequena empresa vende sua lista de clientes a uma empresa de marketing ou dá sua própria lista em troca de outra lista".

A tradução "exploração econômica de dados pessoais", me faz pensar: quais outras interpretações poderiam caber aqui? O quão limitada pode ser uma exploração econômica de dados para não se enquadrar nesta hipótese?

	titular da informação pessoal (access to personal information; e (xiii) correção da informação pessoal pelo titular (correction of personal information) . A Agência Nacional de Proteção de Dados Australiana (*Office of the Australian Information Commissioner*) desenvolveu um manual explicativo (link de acesso abaixo) sobre a interpretação de cada um dos princípios, para que os pequenos negócios sejam capazes de implementá-los na execução dos seus negócios. Interessante notar que não são obrigações prescritivas, mas descritivas de causa e efeito e do objeto a ser tutelado. Esta informação pode ser evidenciada no link: https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/ A informação sobre os APPs pode ser verificada pelo link: https://www.oaic.gov.au/assets/privacy/australian-privacy-principles/the-australian-privacy-principles.pdf CCPA (California Consumer Privacy Act - 2018) A Lei de proteção da privacidade do consumidor da Califórnia, define em uma de suas provisões publicadas, (AB-375) "negócio", isto é, para quem esta lei é aplicável: *(1) Uma empresa individual, sociedade, companhia de responsabilidade limitada, corporação, associação ou outra pessoa jurídica que seja organizada ou operada para o lucro ou benefício financeiro de seus acionistas ou outros proprietários, que colete informações pessoais dos consumidores, ou em nome da qual tais informações sejam coletadas e que sozinha, ou em conjunto com outros, determine as finalidades e os meios de processamento das informações pessoais dos consumidores, que faça negócios no Estado da Califórnia, e que satisfaça um ou mais dos seguintes limites: (A) Tem receita bruta anual superior a vinte e cinco milhões de dólares ($25.000.000), ajustado conforme o parágrafo (5) da subdivisão (a) da Seção 1798.185. (B) Sozinho ou em combinação, compra anualmente, recebe para fins comerciais da empresa, vende, ou compartilha para fins comerciais, sozinho ou em combinação, as informações pessoais de 50.000 ou mais consumidores, domicílios, ou dispositivos. (C) Deriva 50% ou mais de suas receitas anuais da venda de informações pessoais dos consumidores.* **A CCPA, portanto, não se aplica para os negócios que não se enquadram nessas hipóteses!** Esta informação pode ser verificada pelo link: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	A definição de agentes de tratamento de dados não precisa de um critério diferenciado. Aliás, a experiência internacional demonstra que a conceituação se mantém, sendo possível usar o critério já estabelecido no art. 5º, IX da LGPD (controlador e operador), o que deve ter critério especial são as responsabilidades e obrigações do controlador e operador quando se tratarem de Micro, EPP e MEI, conforme ilustra a experiência de outros países.
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)?	Por favor, verificar a informação fornecida para a experiência internacio Ademais, algumas autoridades de proteção de dados europeias, como a I do Reino Unido, têm criado uma série de diretrizes orientativas destinad small businesses e têm adotado uma postura mais educativa do que pun com relação a pequenos negócios. Esta informação pode ser verificada pelos links: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/ https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/frequently-asked-questions/

Comentado [FA4]: Site da Comissão Europeia: pequenas empresas que estejam de acordo com determinados critérios têm direito à benefícios como: menor exigência ou taxas reduzidas para a conformidade administrativa da UE, (além de programas de apoio empresariais diversos).

https://ec.europa.eu/growth/smes/sme-definition_en

Comentado [FA5]: Cartilha online sobre adequação para empresas de pequeno porte da Comissão Europeia: https://ec.europa.eu/justice/smedataprotect/index_en.htm

Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	O cumprimento das obrigações de registro das operações de tratamento não serão observadas pelos agentes de pequeno porte, Micro, EPP e MEI, porque são obrigações de difícil exequibilidade, considerando (i) a complexidade; (ii) o número de empregados dessas empresas; (iii) a falta de qualificação de pessoas com conhecimento específico; (iv) a ausência de exploração de dados sob qualquer forma e (v) o baixo risco de violação da privacidade. O descumprimento implicará em autuações pecuniárias extremamente elevadas para os negócios cuja receita bruta anual alcança o teto máximo de R$ 4,8 milhões, o que demanda a revisão das penalidades para refletir a realidade desses pequenos negócios, para que uma eventual violação não inviabilize um negócio gerador de riqueza e emprego. Penalidades elevadas não estimulam o cumprimento, dada a inexequibilidade da cobrança, ao contrário, se o regime sancionador estiver ao alcance da capacidade financeira, a multa será aplicada e recebida, resultando no caráter corretivo/educativo e preventivo de cumprimento. Importante destacar que o custo de implementação é muito elevado. O Jornal Valor divulgou, em 21.8.2020, uma notícia que diz que a média de custo para a implantação de um projeto que atenda a LGDP varia entre R$ 50 mil e R$ 800 mil, ver notícia: https://valor.globo.com/publicacoes/suplementos/noticia/2020/08/21/custo-da-conformidade-pode-variar-de-r-50-mil-a-r-800-mil.ghtml?GLBID=1a7f1a28b6d8d4c71af4d046ae215d78e55617a6139487a574c796650507a456671456b73565672616f697879534c6f6948374652565751326b34536859476a46494c70774979633937584 26a6576616b46315652574e665a4247617465473275576a694131513d3d3a303a6761627269656c2e66696c686f2e34 Considerando que a receita bruta anual máxima para MEI corresponde a R$ 81 mil; Micro a R$ 360 mil; e EPP a R$ 4,8 milhões, conforme art. 3.º e 18-A da Lei Complementar 123 de 14.12.2006, se tomarmos o valor mínimo de implantação (R$ 50 mil), este custo corresponderia a 61,72 % da receita bruta anual de um MEI; 13,88% para uma Micro; e 1,04% para uma EPP. São percentuais de despesas elevados, o que torna difícil o cumprimento da LGPD como está para os agentes de pequeno porte. Além disso, esta média de custos divulgada se refere à etapa de implementação, ou seja, não estão previstos os custos de manutenção de uma equipe interna ou terceirizada para realizar continuamente o registro das

	operações de tratamento, o que implica em custos fixos adicionais aos agentes de pequeno porte, onerando demasiadamente os pequenos negócios, sem que haja a correlata exposição de riscos à proteção da privacidade.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	O primeiro impacto é a ausência de necessidade, em decorrência da ausência de exploração econômica dos dados. Se a atividade empresarial do agente de pequeno porte não envolve a exploração de dados sob qualquer hipótese, ter um agente é desnecessário. A segunda razão, são os custos de pagamento de um encarregado, seja como empregado, seja como prestador de serviços, por este motivo, sugerimos que as Micro, EPP e MEI indiquem uma pessoa como representante legal para contato pela ANPD, se necessário, mas sem a necessidade de ser especialista.
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	O impacto é o alto custo da elaboração de um relatório de impacto à proteção de dados frente aos riscos da atividade (alto custo *vs* risco baixo). Este relatório identificará um risco baixo, que pela própria descrição das atividades poderia ser identificado, já que tais empresas não fazem a exploração econômica de dados pessoais, deixando de ter sentido esta atividade aos agentes de pequeno porte. Importante destacar a experiência australiana, que criou um questionário para verificar se o small business está obrigado ou não ao cumprimento da Privacy Act 1988.

Comentado [6]: Uma pesquisa da Cisco: "Data Privacy Benchmark Study- 2021", sobre os custos de investimento em privacidade para organizações menores (250-499 funcionários). O orçamento médio cresceu de US$ 0,8 milhões para US$ 1,6 milhões, em comparação com o ano anterior.

	O teste pode ser verificado pelo link: https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/#PrivacyChecklistForSmallBusiness Sugerimos aproveitar esta experiência de um teste de aderência, disponível numa plataforma pública, cujas informações poderão ser arquivadas como uma autodeclaração da condição de agente de pequeno porte.
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?	O tratamento de dados em si tem um custo muito elevado, como já justificado. Os dados sensíveis e de crianças e adolescentes, quando utilizados exclusivamente para o cumprimento de uma obrigação contratual pelos agentes de pequeno porte, deveriam ter o mesmo tratamento dos dados pessoais gerais, na forma da regulamentação específica a ser elaborada para este fim.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	O impacto da implementação de um programa de governança de dados **proporcional** aos agentes de pequeno porte, com medidas de proteção suscetíveis de cumprimento, que sejam **declaratórias e comportamentais**, não onerando e criando novas e contínuas despesas é possível e recomendável.

Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	A implantação de uma política de segurança relativa à proteção de dados pessoais, desde que **proporcional** à atividade do pequeno negócio e aos riscos que possam causar, é possível e recomendável. Nesse sentido, a ANPD pode criar um padrão técnico, considerando comportamentos comuns e regulares praticados por MEI, Micro e EPPs, a exemplo da recomendação de criação de códigos de conduta pela GDPR e os 13 princípios australianos, a ANPD em associação com entidades de classe pode criar códigos específicos que recomendam aspectos da política de segurança e das medidas de governança.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	A avaliação sistemática de riscos é medida excessiva para agentes de pequeno porte que não explorem dados com fins econômicos. Ela só deveria ser obrigatória se o agente de pequeno porte alterar o uso dos dados, mas se não os explora e os utiliza apenas para cumprir a obrigação para o qual foi contratado, a avaliação é medida extremamente onerosa.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	A portabilidade de dados é relevante e deverá ter um tratamento específico, porque muitos MEIs, Micro e EPPs recebem dados portados para cumprimento das obrigações contratuais, assim, devem cumprir as próprias obrigações e não serem obrigados a cumprir obrigações mais onerosas. Por regra, a portabilidade não deve alterar as obrigações especiais dos agentes de pequeno porte.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de	A exemplo da lei tributária, que busca simplificar e desonerar os empreendedores individuais, as micro e as empresas de pequeno porte, no âmbito da proteção de dados pessoais também deverá existir uma **LGPD-Simples**.

pequeno porte?	
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Tomada de Subsídios 1/2021

institucional@faciap.org.br

qua 24/03/2021 16:53

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

1 anexo

CONTRIBUIÇÕES - ANPD - TRATAMENTO DIFERENCIADO.pdf;

Prezados, boa tarde

A **FEDERAÇÃO DAS ASSOCIAÇÕES COMERCIAIS E EMPRESARIAIS DO ESTADO DO PARANÁ**, pessoa jurídica de direito privado regularmente inscrita no CNPJ sob nº 40.312.993/0001-51, com sede à Rua Heitor Stockler de França, 356, Centro Cívico, CuriÃba, PR, CEP 80.030-030, neste ato representada por seu presidente **FERNANDO MAURICIO DE MORAES**, brasileiro, casado, portador da Cédula de Iden. dade nº 5434537-2/PR e inscrito no CPF/MF sob nº 677.850.779-91, vem, através do presente o. cio, apresentar sugestão de regulamento de tratamento diferenciado e procedimento simplificado de adequação da lei geral de proteção de dados pessoais para as microempresas e empresas de pequeno porte, bem como inicia va empresariais de caráter incremental ou disrup vo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme documento em anexo.

Nos colocamos à disposição para eventuais esclarecimentos.

Sem mais, nossos mais elevados votos de es ma e consideração.

FERNANDO MAURICIO DE MORAES
PRESIDENTE DA FACIAP

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: FEDERAÇÃO DAS ASSOCIAÇÕES COMERCIAIS E EMPRESARIAIS DO ESTADO DO PARANÁ – FACIAP

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

CONSIDERANDO que a FACIAP, entidade integrante do G7[1], representa hoje 290 associações comerciais e um universo de mais de 50 mil empresas em todo o Estado.

CONSIDERANDO que a FACIAP é uma das maiores instituições do sistema no Brasil, com atuação em 75% dos municípios paranaenses.

CONSIDERANDO que a FACIAP visa defender os interesses empresariais, ao promover o desenvolvimento sustentável das associações comerciais e do sistema associativista, com solução em produtos e serviços, contribuindo para a competitividade do estado do Paraná.

CONSIDERANDO que a FACIAP é a porta-voz do empresariado paranaense junto aos governos municipal, estadual e federal, além de entidades privadas que interferem na ação das empresas.

CONSIDERANDO que todas as pessoas jurídicas deverão se adequar à Lei nº 13.709/2018 – LGPD - Lei Geral de Proteção de Dados, e que é de interesse, e, dever, da FACIAP auxiliar as suas filiadas para que se adequem à referida lei.

[1] G7- Grupo formado pela Federação das Indústrias do Paraná (Fiep), Federação da Agricultura do Paraná (Faep), Federação e Organização das Cooperativas do Paraná (Fecoopar), Federação do Comércio do Paraná (Fecomércio-PR), Federação das Empresas de Transporte de Cargas do Paraná (Fetranspar), Associação Comercial do Paraná (ACP), Federação das Associações Comerciais e Empresariais do Estado do Paraná (Faciap) e Sebrae-PR.

CONSIDERANDO o art. art. 55-J, XVIII, da Lei nº 13.709, que prevê compete à ANPD 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 LGPD.

CONSIDERANDO que a Nota Técnica nº 1/2021/CGN/ANPD, visa obter subsídios, informações e dados relevantes dos agentes econômicos, consumidores e demais interessados da sociedade, para regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

A **FEDERAÇÃO DAS ASSOCIAÇÕES COMERCIAIS E EMPRESARIAIS DO ESTADO DO PARANÁ**, pessoa jurídica de direito privado regularmente inscrita no CNPJ sob nº 40.312.993/0001-51, com sede à Rua Heitor Stockler de França, 356, Centro Cívico, Curitiba, PR, CEP 80.030-030, neste ato representada por seu presidente **FERNANDO MAURICIO DE MORAES**, brasileiro, casado, portador da Cédula de Identidade nº 5434537-2/PR e inscrito no CPF/MF sob nº 677.850.779-91, vem, através do presente ofício, apresentar:

SUGESTÃO DE REGULAMENTO DE TRATAMENTO DIFERENCIADO E PROCEDIMENTO SIMPLIFICADO DE ADEQUAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS PARA AS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE, BEM COMO INICIATIVA EMPRESARIAIS DE CARÁTER INCREMENTAL OU DISRUPTIVO QUE SE AUTODECLAREM STARTUPS OU EMPRESAS DE INOVAÇÃO E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS COM FINS ECONÔMICOS

CONTRIBUIÇÕES

A Lei Geral de proteção de Dados foi inspirada na GDPR - General Data Protection Regulation (Regulamento Geral de Proteção de Dados) da União Europeia, que prevê que o direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

Conforme consta na GDPR, há uma "derrogação" para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além as autoridades de controle, são incentivadas a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação da referida Lei.

A GDPR prevê ainda que esta não se aplica ao tratamento de dados pessoais efetuado por pessoas **singulares** (físicas) no exercício de atividades exclusivamente pessoais ou domésticas. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrônico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

Atualmente, a LGDP dispensa o tratamento de dados pessoais por pessoas naturais sem finalidade econômica, desta forma, toda pessoa física com finalidade econômica deverá realizar o tratamento de dados pessoais conforme as previsões da LGPD, contudo, entende-se necessário enumerar ou exemplificar quais pessoas físicas enquadram-se nesta hipótese ou qual o entendimento de finalidade econômica, seria no viés de profissionais liberais? Autônomos? Ou apenas pessoas físicas que "comercializem dados pessoais"?! Obviamente, estas pessoas possuem finalidade econômica, entretanto, condicionar que um autônomo realize o tratamento de dados pessoais da mesma forma que uma empresa "normal" não faz sentido.

Importante destacar que antes mesmo da entrada em vigor da GDPR, o México já possuía a chamada "LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES", que também prevê exceção no tratamento de dados pessoais para as pessoas que procedem à recolha e armazenamento de dados pessoais, para uso exclusivamente pessoal, e sem fins de divulgação ou **utilização comercial.**

Desta forma, considerando a abrangência do termo "finalidade econômica" a sugestão é que o termo "finalidade econômica" seja substituído para "utilização comercial".

Além da hipótese de tratamento por pessoas físicas com finalidades econômicas, a LGDP impõe a adequação por parte das microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação.

Entretanto, a lei prevê que compete à ANPD a 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 LGPD. Cumpre informar, que é necessário que este tratamento diferenciado seja disponibilizado também para os Microempreendedores Individuais.

Pois bem, a própria lei já trouxe esta previsão justamente por se tratar de empresas que possuem um porte "menor" e consequentemente menos recursos que uma grande multinacional por exemplo. Sendo em sua maioria, pequenas empresas familiares. Inclusive estas empresas já possuem tratamento diferenciado perante as Leis Complementares 123/2006 e 167/2019), razão pela qual, a necessidade de a LGPD acompanhar as demais legislações.

Necessário destacar que se considera microempresa ou empresa de pequeno porte, a sociedade empresária, a sociedade simples, a empresa individual de responsabilidade limitada e o empresário que exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que: (Art. 3º da Lei Complementar 123/2006)

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).

E ainda, importante que a ANPD estabeleça, o tratamento diferenciado para empresas citadas acima, de acordo com o seu porte e número de colaboradores registrados na empresa. Ex. até 20 colaboradores Microempresa, de 21 a 70 – médio porte.

No que tange as Start-ups, 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. (art. 65-A, §1º da Lei Complementar 167/2019).

Diante do exposto, necessário se faz a regulamentação do tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

Dentre outros tratamentos, espera-se, entre outras medidas, que as empresas acima citadas possuam prazos diferenciados para atendimento das solicitações dos titulares, bem como, para eventuais comunicações de incidentes com dados pessoais à ANPD, tratamento diferenciado quando da aplicação das penalidades pela ANPD.

Destaca-se ainda a necessidade de a ANPD:

a) Emitir uma nota técnica sobre o entendimento dos dados dos representantes legais de empresas, pois conforme a LGPD, os dados de pessoa jurídica não são compreendidos pela LGPD, e o entendimento desta Entidade é que os dados de representante legais, embora sejam pessoas físicas, não estariam regidos pela LGPD, pois trata-se de dados da pessoa jurídica.

b) Regulamentar para quais hipóteses enquadra-se o tratamento de dados pessoais na base legal “Legitimo Interesse do Controlar”, visto que o termo pode levar à diversos entendimentos por parte dos agentes de tratamento de dados e até mesmo ser confundido com a base legal do consentimento nos casos de apoio e **promoção de atividades** do controlador (art. 10, I da LGPD). Bem como, incluir no art. 7,VI, a previsão do exercício regular do direito em processo de mediação nos termos da Lei 13.140/2015.

c) Regulamentar qual a melhor forma de as empresas confirmarem que o solicitante de informações acerca de seus dados é de fato o titular do dado, tendo em vista a fragilidade das fraudes ocorrerem por meios eletrônicos e telefônicos.

d) Dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

e) Dispor sobre padrões técnicos mínimos para o tratamento de dados pessoais para as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais.

f) Regulamentar o tratamento de dados pessoais de adolescentes, visto que o art. 14, I, prevê apenas o consentimento dos pais ou representante legal no tratamento de dados pessoais de crianças. E, de acordo com o Estatuto da Criança e do Adolescente, considera-se criança, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Diante do exposto, a FACIAP reitera as sugestões de redação de cláusulas realizadas pelo SEBRAE - Serviço Brasileiro de Apoio às Micro e Pequenas Empresas, bem como, aproveita para incluir as seguintes cláusulas como sugestão para o tratamento diferenciado das empresas citadas:

REGULAMENTO – ANPD

Art. 1º Este regulamento estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às para as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais.

Art. 2º Para os efeitos deste regulamento, 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: (Redação dada pela Lei Complementar nº 123, de 2016)

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 com até 20 colaboradores registrados na empresa.

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) e com até 70 colaboradores registrados na empresa.

Art. 3º - Considera-se pessoa física com finalidade comercial aquela que promova a oferta de bens e serviços.
§ Não se enquadram nesta hipótese as pessoas físicas para fins deste regulamento, as pessoas que realizam o tratamento de dados pessoais conforme determinação de um Controlador.

Art. 4º 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. (Redação dada pela Lei Complementar 167/2019).

Art. 5º O regime diferenciado e simplificado de obrigações instituídas neste regulamento tem por objetivo:

I – Reconhecer que as empresas e pessoas físicas referidas nos arts. 2º,3º e 4º, encontram-se em situação de desequilíbrio perante o conjunto de obrigações trazidas pela LGPD;
II – Ampliar a efetividade dos preceitos da LGPD, tornando o cumprimento das obrigações nela previstas exequíveis às microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais;
III – privilegiar a presunção de boa-fé, nos termos do art. 3º, V, da Lei nº 13.874, de 20 de setembro de 2019, e o caráter precipuamente educativo da legislação de proteção de dados pessoais às microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais;
IV – Conferir tratamento isonômico aos agentes de tratamento de dados pessoais que se enquadrem nas condições aqui previstas.

Prazos diferenciados para o atendimento às solicitações dos titulares de dados pessoais

Art.6º Os prazos para as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais atenderem às solicitações dos titulares referentes ao tratamento de seus dados pessoais são ampliados para sessenta dias. (Art. 19, da LGDP)

Parágrafo único. Em até 15 dias após a solicitação, as empresas e/ou pessoas físicas deve informar o titular dos dados sobre a confirmação da existência de tratamento.

Prazos diferenciados e formulários simplificados para a comunicação de incidentes à ANPD

Art. 7º O prazo para as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais comunicarem à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48 da LGPD) é de dez dias úteis após seu conhecimento.

§ 1º É dispensada a comunicação se o incidente não resultar em risco para os direitos e liberdades dos titulares.

§ 2º Se a notificação à ANPD não for realizada no prazo do *caput*, deve ser acompanhada dos motivos do atraso.

§ 3º A comunicação à ANPD deve ser feita por meio de formulários eletrônicos simplificados, que reduzam o custo financeiro e de tempo para o preenchimento, e preferencialmente, através de peticionamento eletrônico no Sistema Eletrônico de Informações – Usuário Externo.

Prazo para a resolução de controvérsias

Art. 8º A fim de estimular a resolução consensual de controvérsias, as petições do titular dos dados contra as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais só serão apreciadas pela ANPD se a reclamação direta à controladora não tiver sido solucionada no prazo previsto no art. 7º.

Condições para a dispensa de obrigações previstas na LGPD

Art. 9º As microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais que se enquadrem nas condições deste regulamento, estão dispensadas de cumprir as seguintes obrigações:

I – Manter registro das operações de tratamento de dados pessoais que realizarem (art. 37 da LGPD), inclusive quando a base legal utilizada for o legítmo interesse do controlador;
II – Elaborar relatório de impacto à proteção de dados pessoais referente às suas operações de tratamento de dados (art. 38 da LGPD), inclusive quando exceto quando a operação de tratamento apresentar alto risco para os direitos e liberdades dos titulares, na forma definida pela ANPD em regulamento específico;
III – indicar encarregado pelo tratamento de dados pessoais (art. 41 da LGPD);
IV – Adotar medidas técnicas e administrativas aptas desde a fase de concepção do produto ou serviço até sua execução (art. 46, § 2º, da LGPD);
V – Anonimizar ou pseudonimizar os dados pessoais.
VI – Realizar a operação de portabilidade

§ 1º O Microempreendedor individual é dispensado de indicar encarregado pelo tratamento de dados pessoais, ainda que não se enquadre nas condições previstas neste regulamento.

§ 2º As microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais devem adotar medidas simplificadas de segurança e que sejam proporcionais ao risco do negócio, podendo a ANPD indicar quais as medidas a serem adotadas.

§ 3º A ANPD, em caso de suspeita de tratamento de dados pessoais que apresente risco aos titulares, pode solicitar relatório de impacto à proteção de dados pessoais, com prazo de atendimento superior em trinta dias ao maior prazo concedido a outros agentes de tratamento.

§4º As empresas e/ou pessoas físicas poderão coletar dados de crianças e adolescentes sem o consentimento dos pais ou representantes legais, quantas vezes forem necessárias para a sua proteção, podendo replicar para Autoridades que defendam o interesse dos direitos das crianças e adolescentes. (art 14§3º da LGPD) Ex: Conselho Tutelar

Atendimento das solicitações dos titulares de dados

Art. 9º As microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais podem atender às requisições dos titulares de dados pessoais, descritas no artigo 18 da LGPD, pelo meio que entenderem mais conveniente, seja ele eletrônico, telefônico, presencial ou impresso.

§ 1º Se o titular exigir a resposta por meio impresso em sua requisição, poderá ser cobrado dele os custos relativos à impressão e postagem, podendo inclusive condicionar o atendimento da solicitação à comprovação do pagamento.

§ 2º As MPEs ficam dispensadas do envio da declaração a que se refere o art. 19, II, da LGPD.

Dispensa de obrigação específica de divulgar informações sobre o tratamento de dados pessoais

Art. 10º As microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais estão dispensadas de divulgar informações sobre o tratamento de dados pessoais em sítio eletrônico, podendo fazê-lo diretamente mediante comunicação ao titular ou por meios alternativos, como correio eletrônico, conta em rede social, aplicativo de mensagens, ou qualquer outra forma que permita a comunicação direta entre estas e o titular de dados pessoais.

Parágrafo único. A gestão do consentimento do titular de dados pessoais de que tratam os arts. 8º e 9º da LGPD também pode ser feita pelos meios descritos no *caput.*

Programa simplificado de governança em privacidade e proteção de dados pessoais

Art. 11. As empresas e/ou pessoas físicas podem estruturar programa simplificado de governança em privacidade e proteção de dados pessoais, nos termos do artigo 50, §2º, I, da LGPD.

§ 1º O programa simplificado deve priorizar:

I – o efetivo respeito aos direitos dos titulares dos dados pessoais;
II – a realização de ações educativas sobre privacidade e proteção de dados pessoais; e
III – a construção de uma política de privacidade que respeite os princípios do art. 6º da LGPD.

§ 2º O MEI é dispensado de estruturar programa simplificado de governança em privacidade e proteção de dados pessoais.

Etapa prévia educativa

Art. 12. Antes da aplicação das sanções previstas no art. 52 da LGPD, a ANPD deve adotar etapa educativa e de orientação às empresas e pessoas fiscais aqui estabelecidas, com indicação de prazo para adoção de medidas corretivas. Bem como, deverá fomentar as formas de autocomposição de conflitos, tais como a conciliação, mediação.

§ 1º A orientação deve elencar as adequações e medidas a serem adotadas, bem como fixar prazo razoável para o seu cumprimento.

§ 2º Caso a etapa educativa e de orientação descrita no *caput* já tenha sido aplicada às empresas e pessoas físicas nos últimos doze meses da data da ocorrência da nova infração, a ANPD deve aplicar a penalidade de advertência (art. 52, I, da LGPD) antes de qualquer outra sanção descrita no artigo.

§ 3º A reincidência da empresa e/ou pessoa física em qualquer infração relacionada à LGPD dentro do período de doze meses não permite a invocação do tratamento diferenciado previsto no *caput*.

Penalidades

Art. 13. As multas aplicadas pela ANPD com base no art. 52, II e III, da LGPD, e na ausência de previsão normativa de valores específicos e mais favoráveis para as empresas, sofrem redução de:

I – Noventa por cento para os Microempreendedores individuais, startups e as pessoas físicas que tratam dados com finalidade comercial;
II – Cinquenta por cento para as microempresas ou empresas de pequeno porte.

Parágrafo único. As reduções de que tratam os incisos I e II do *caput* não se aplicam se comprovada qualquer das seguintes situações:

I – fraude, resistência ou embaraço à fiscalização;
II – inadimplemento superior a noventa dias no pagamento de outra multa imposta pela ANPD.

Parágrafo único. As multas aplicadas podem ser parceladas em prazos maiores do que os concedidos a outros agentes de tratamento.

Termo de compromisso

Art. 14. Nos termos do artigo 26 do Decreto-Lei nº 4.657, de 4 de setembro de 1942, a ANPD pode celebrar termo de compromisso com as empresas e/ou pessoa físicas infratoras, no qual esta se obrigue a, cumulativamente:

I - cessar a infração à LGPD sob investigação ou os seus efeitos lesivos;
II - corrigir as irregularidades apontadas e indenizar os prejuízos aos titulares de dados pessoais;
III - cumprir as demais condições que forem acordadas no caso concreto.

§ 1º O termo de compromisso pode prever cláusula penal para as hipóteses de:

I – total ou parcial inadimplemento das obrigações compromissadas;
II – mora do devedor;
III – garantia especial de determinada cláusula.

§ 2º O termo de compromisso não importa confissão quanto à matéria de fato, nem reconhecimento da ilicitude da conduta analisada.

§ 3º Durante a vigência do termo de compromisso, os prazos de prescrição de que trata a Lei nº 9.873, de 23 de novembro de 1999, ficam suspensos, e o procedimento administrativo deve ser arquivado se todas as condições nele estabelecidas forem atendidas.

§ 4º O cumprimento das condições do termo de compromisso gera efeitos exclusivamente na esfera de atuação da ANPD.

Vigência

Art. 15. Este regulamento entra em vigor na data de sua publicação.

Interpretação e resolução de dúvidas

Art. 16. A ANPD pode emitir atos declaratórios para esclarecer eventuais dúvidas decorrentes da interpretação ou da aplicação deste regulamento, ouvidas as entidades representativas das microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins comerciais.

Tomada de Subsídios 1/2021 - complemento de subsídios

Marcelo Fattori [redacted]

qua 03/03/2021 13:59

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

[redacted]

2 anexos

lgpd_facil_seusdados_contribuicoes_PME_5-2-21.pdf; marcelo augusto fattori - curriculo lattes.pdf;

Ilustríssimo(a) Senhor(a), boa tarde!

Em complemento a correspondência anterior onde solicitamos parcipaç ão da tomada de subsídios para parcipaç ão de agenda com membro desta i. ANPD., apresentamos com o devido acatamento nossa contribuição sobre o tema da regulação para pequenas e microempresas, a parr da nossa eąxperiência em dezenas de projetos de conformidade realizados e em curso, bem como a parr da eąxperiência acadêmica no Brasil e na Europa.
Estamos à disposição para qualquer contribuição necessária.
Atenciosamente,

Marcelo Fattori
marcelo@seusdados.com
+55 11 97509 0509 ☎ +55 11 4587 2900
seusdados

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: LGPD FÁCIL SERVIÇOS VIRTUAIS LIMITADA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	A proteção de dados pessoais e o respeito à privacidade, de longe não é o coração da atividade empresarial de qualquer porte de empresa, exceto aquelas que tem esse escopo de atuação.

	Nossa consultoria, há dois anos, atua de forma multidisciplinar e em formato digital, apoiando empresas na execução dos seus programas de conformidade com as normas de proteção de dados pessoais e privacidade. Nossa base de conhecimento teórico, de profissionais que integram grupos de pesquisa em universidade de renome, com formação na União Europeia em proteção de dados, aliado à base de conhecimento prática construída ao longo desses anos apoiando empresas de todos os segmentos de atuação, permitiu detectar fatos que devem ser considerados no desenvolvimento do ambiente nacional de regulação em proteção de dados, dentre as quais, ousamos pontuar, como contribuição para esse d. órgão e para a sociedade em geral: 1. Em primeiro lugar, para que seja possível a tomada de decisão sobre rumos de regulação da proteção de dados pessoais no âmbito de profissionais liberais e das pequenas empresas, necessário delinear a realidade atual de mercado para compreensão das dificuldades a serem enfrentadas nesse processo; 2. De acordo com o DATASEBRAE[1], com dados da Receita Federal do Brasil (RFB) de 11.5.2020, o Brasil conta com 19.228.025 empresas, sendo que desse total 85% (oitenta e cinco por cento) equivalentes a 16.396.980 referem-se a microempresas (ME) e microempreendedor individual (MEI). Quando somados a esse montante as empresas de pequeno porte (EPP), temos um total de 17.293.316 representando 90% (noventa por cento) das empresas brasileiras. 3. Essa informação é fundamental para compreensão de que não haverá sistema de proteção de dados eficiente em nosso país, se não houver especial atenção e regulação para o referido tipo de empresas. 4. Da mesma forma resta claro ser impensável qualquer tipo de dispensa do cumprimento das normas de proteção de dados para profissionais liberais, MEI´S, ME´s e EPP´s, sob pena de perecimento da ideia de criação de um sistema de proteção de dados no Brasil. 5. A pesquisa acima demonstra, ainda, que do ponto de vista da proteção de dados pessoais não há como olhar para profissionais liberais, MEI´S, ME´s e EPP´s, a partir das mesmas premissas e critérios que serão aplicados para empresas de médio e grande porte, o que revela a sensatez desse órgão regulador ao buscar a oitiva da comunidade brasileira sobre o tema. 6. Na mesma linha, o desenvolvimento tecnológico é uma nova realidade de mercado, com o surgimento de *startups*, que possuem estrutura física, de pessoal e até mesmo

[1] SEBRAE. Total de Empresas. Disponível em: https://datasebrae.com.br/totaldeempresas/. Acesso em 05.02.2021.

	de faturamento na maioria dos casos não tão relevantes, mas que manuseiam, em razão do modelo de negócio, milhares de dados pessoais, na construção de seus bancos de informações, na disponibilização de serviços e nos acessos que recebem em seus *sites* da internet por usuários interessados em produtos e serviços disruptivos, em muitos casos sem a aplicação das boas práticas de gestão e segurança dos dados pessoais. 7. Além das organizações até aqui mencionadas, não se pode ignorar a diversidade de cultura e a dimensão do nosso território, que impactam sobremaneira no tema em comento. Um morador de um grande centro, conhecedor dos seus direitos e das obrigações das empresas quanto a observância da LGPD, pode não encontrar em um pequeno comércio do interior do Brasil, onde está visitando, a esperada atenção a esse regramento, posto que a prática e a cultura local, não exigem esse comportamento, fato que se ignorado pelo órgão regulador e fiscalizador poderá representar injustiça para os dois lados. 8. Esse desafio precisa ser pensado para além do texto legal, sem que isso represente, obviamente, descumprimento da lei, para contemplar a todos os personagens desse ambiente um sentimento de segurança jurídica que viabilize negócios e garantam os direitos fundamentais do titular de dados. 9. Outro ponto identificado pela nossa consultoria, foi a existência de um número extremamente relevante de empresas Brasil a fora que operam apenas em modo físico, com coleta e armazenamento de dados pessoais, documentos de identificação, pastas de arquivo, livros e cadernos com informações de colaboradores, visitantes, doadores, pacientes, clientes, enfim, pessoas relacionadas ao dia a dia da sua operação, sem qualquer atenção a medidas de segurança da informação, tampouco possuem nesse modelo capacidade de atender aos direitos do titular de dados, nos termos da LGPD, haja vista que sequer têm condições de identificar onde, como e porque estão na posse de referidos dados. 10. As recentes crises financeiras e a pandemia do Coronaovírus, após um período de crescimento econômico, tornaram ainda mais desafiador tratar da proteção de dados visto que, se por um lado as empresas tiveram que buscar implementar soluções de atendimento virtualizado e remoto, valendo-se cada vez mais de dados pessoais do titular para atender as necessidades desse novo modelo de negócio, por outro lado, tais soluções vêm sendo adotadas diante da escassez de recursos financeiros e da ausência de uma cultura de segurança da informação e compreensão do impacto que

	o uso indevido de tais informações podem gerar para o titular, sem a devida atenção aos procedimentos de boas práticas em gestão e governança de dados. 11. A que se observar, ainda, que a dificuldade imposta pela pandemia não é o fator preponderante para a ausência de providências no âmbito da LGPD por tais organizações. O que pudemos notar durante o período de *vacatio legis* foi a descrença generalizada sobre a entrada em vigor da lei e sua efetividade, bem como sobre a forma de atuação do órgão regulador, o que desmotivou empresários a realizar seu processo de conformidade no prazo de dois anos entre a promulgação da lei e sua entrada em vigor; 12. Nesse período, buscaram adaptar suas estruturas às normas de proteção de dados as empresas nacionais de médio e grande porte, bem como aquelas que possuíam relação comercial ou societária com o mercado externo que exigiam o cumprimento de processos relativos à proteção de dados em razão das leis estrangeiras. Ainda assim, a grande maioria das grandes corporações ainda não iniciaram seu processo de aderência à LGPD, conforme pesquisa da Associação Brasileira de Normas Técnicas (ABNT)[2] dando conta de que apenas 12% (doze por cento) das empresas atenderam mais de 61% dos requisitos da LGPD. 13. Referida pesquisa aponta ainda, que 53% das empresas entrevistadas estimam gastar até R$100 mil, e 15% estimam gastar até R$500 mil, em seus programas de adequação. 14. Some-se aos altos custos envolvidos na adaptação das empresas para garantir a devida segurança da informação e estabelecer os processos de conformidade, a ausência de recursos reservados tanto, bem como a realidade de que profissionais liberais, MEI´S, ME´s e EPP´s possuem estruturas de pessoal enxuta, quando não operam individualmente, e não dispõem de pessoas especializadas para desenvolver o programa de conformidade, tampouco para gerenciar a tecnologia e segurança da informação, valendo-se de serviços pontuais de terceiros, que sofrem das mesmas dificuldades, o que cria um círculo vicioso de tratamento e compartilhamento de dados pessoais ao arrepio do mínimo desejável em proteção dos dados pessoais pela LGPD, e que representa um anseio da sociedade como um todo. 15. Para agravar o desafio, não se pode perder de vista a obrigatoriedade de um sistema hermético de proteção de dados, baseado no conceito de *enforcement*, onde a vulnerabilidade de qualquer das partes da cadeia de produção, fornecimento e

[2] ALVAREZ e MARSAL. DISPUTES AND INVESTIGATIONS CYBER RISK SERVICES. Associação Brasileira de Normas Técnicas: 2020. Disponível em: http://www.abnt.org.br/images/Docspdf/Alvarez_e_Marsal_Pesquisa_de_Maturidade_da_LGPD.pdf. Acesso em: 05 fev. 2020.

	distribuição de produtos e serviços, implicará na vulnerabilidade dos demais parceiros de negócio. 16. Sendo os profissionais liberais, MEI´S, ME´s e EPP´s, os mais relevantes parceiros de negócio das médias e grandes corporações, a conformidade destas depende do atendimento dos comandos legais por aquelas. 17. Esse retrato sintetizado da proteção de dados, demonstra que não teremos um ambiente seguro e internacionalmente reconhecido quanto a proteção de dados se não houver um olhar imediato, atento e viabilizador de regulações apropriadas para profissionais liberais, MEI´S, ME´s e EPP´s criarem a cultura de proteção de dados e efetivamente implementá-las para estarem em conformidade com a LGPD. 18. Isso somente ocorrerá se a Autoridade Nacional de Proteção de Dados (ANPD), fazer prevalecer o verdadeiro senso de justiça preconizado por Ruy Barbosa[3], ou seja, de tratar igualmente os iguais e desigualmente os desiguais, na medida da sua desigualdade. As considerações tratadas acima, são as premissas para que possamos pontuar objetivamente os desafios para regular a proteção de dados para profissionais liberais, MEI´S, ME´s e EPP´s, que passamos a destacar: **Desafios estruturais:** i. Ausência de conhecimento da população brasileira e do setor empresarial sobre o que efetivamente sejam dados pessoais no contexto da LGPD; ii. Desconhecimento sobre a repercussão do uso indevido e as consequências de incidentes de segurança com dados pessoais; iii. Cultura de coleta massiva e invasiva de dados pessoais independentemente da existência de finalidade específica; iv. Prática atual de mercado que massacra o consumidor com o pedido de dados pessoais sem qualquer relação com o tema, que acuado em uma relação desigual acaba por fornecer, ainda que contra sua vontade suas informações; v. Não aplicação de dispositivos legais sobre uso inadequado de dados previstos no âmbito do Código de Defesa do Consumidor e do Marco Civil da Internet, tendo como consequência da ausência de uma política de conscientização, fiscalização e penalizações o desestimulo do seu cumprimento;

[3] BARBOSA, Ruy. Oração aos Moços. Disponível em: https://www.literaturabrasileira.ufsc.br/_documents/0006-01488.html. Acesso em: 05 fev. 2020.

	vi. Esse histórico aliado à prática por parte de grandes corporações de tratamento abusivo dos dados pessoais sem qualquer repressão, incentivou a difusão da ideia absolutamente equivocada de que a LGPD seria uma lei que “não pegaria”. vii. O desconhecimento por parte de profissionais liberais sobre as reais finalidades e usos dos dados compartilhados com parceiros de negócio, vide exemplo do que ocorre na relação entre médicos e determinados laboratórios, planos e seguros de saúde. Para o médico o tratamento dos dados pessoais do paciente limita-se, ressalvadas ações indevidas, a atenção à sua saúde. Por seu turno, algumas empresas da área de saúde, podem ter outras finalidades no tratamento dos dados recebidos do referido profissional, para além do atendimento à saúde daquele paciente, ligadas à melhoria da sua performance financeira, a monetização da informação, sem que isso seja de conhecimento dos demais envolvidos nesse processo; viii. Nada obstante relevante avanço nos últimos anos, ainda é um desafio a ausência de transparência nas relações negociais; ix. Baixa escolaridade e nível cultural indesejado da grande massa de mão de obra, que não está apta para zelar pelo tratamento diligente e seguro de informações relevantes, caso dos dados pessoais; x. Conflito de valores entre gerações de gestores e empresários desconectados com as novas demandas de uma geração digital, com exigências voltadas para governos e empresas que atendam o ideal de consumo e desenvolvimento sustentável e atendimento a demandas regulatórias; xi. O amplo acesso da população brasileira à internet e mídias sociais, apesar do completo desconhecimento sobre os riscos das atividades em ambiente em rede; xii. Cultura de que a observância de normas, o investimento em conscientização e segurança, representa despesa e, consequentemente, prejuízo ou perda de competitividade, especialmente em um modelo de mercado baseado no conhecimento das pessoas, seus hábitos, predileções, perfis de consumo, dentre outras; xiii. Maior questionamento que recebemos diz respeito a insegurança em investir em processos decorrentes de medidas e leis que exigem adaptações do empreendedor e que são revogadas após investimentos e adaptações geralmente custosas, caso típico do e-social, e outras ações no âmbito das obrigações fiscais/contábeis;

	xiv. Empresas, comércios, prestadores de serviços e profissionais liberais que não possuem fluxos e processos definidos no seu negócio; xv. Alto custo do acesso à rede mundial de computadores. O Brasil é a nação com a 58ª internet mais cara do mundo[4], e de baixa eficiência; xvi. Alto custo das ferramentas e soluções de tecnologia, geralmente precificada em dólar norte americano; xvii. Ausência de política pública de incentivo para fomentar a cultura de investimento e adequação do parque tecnológico com equipamentos, ferramentas e soluções de tecnologia e segurança da informação, acessíveis, amigáveis e que não impliquem em dificuldades no desenvolvimento da atividade empresarial e não impactem o capital de giro necessário para manutenção do negócio; xviii. Escassez de recursos privados para investimento em equipamentos e ferramentas e soluções de tecnologia e segurança da informação; xix. Ausência de estratégias e políticas públicas voltadas para o mercado financeiro comercializar produtos de financiamento para aquisição de equipamentos e ferramentas e soluções de tecnologia e segurança da informação; xx. Ausência de política pública voltada para a educação do uso ético e adequado da tecnologia; xxi. Custos elevados para geração de evidências sobre fatos ocorridos na empresa, como os altos custos de atas notariais, que têm custos aproximados de R$400,00 para primeira folha e R$200,00 para as demais, o que é proibitivo para o microempreendedor; xxii. As demandas decorrentes de fatos ocorridos no ambiente digital dependem de custódia da prova, que quando submetida a apreciação do Poder Judiciário tem valor relativizado, e o empreendedor tem que desembolsar valores altos para perícias, nem sempre de boa qualidade técnica, o que o afasta do Poder Judiciário e da solução dos conflitos; xxiii. Poder Judiciário não estruturado para solucionar na ponta, nas milhares de comarcas, onde as provas são produzidas, as demandas no ambiente digital, por ausência de aparato tecnológico apropriado e pessoal especializado para apoiar tecnicamente o magistrado; xxiv. Morosidade das soluções judiciais que tornam ineficazes as decisões de casos que tenham relação com o ambiente digital onde a informação é propalada em velocidade;

[4] https://www.tecmundo.com.br/internet/149557-brasil-58-ranking-internet-cara-no-mundo.htm

	xxv. xxvi. xxvii.
Existem sugestões para endereçamento do problema?	**Sim, e de início afirmamos que não haverá ambiente de proteção de dados no Brasil e a LGPD será vazia, se afastado o microempreendedor, o profissional liberal, da obrigatoriedade do seu cumprimento.** **Empresas não irão a falência por cumprir regras. Pessoas podem ter suas vidas devastadas pelo descumprimento de regras pelas empresas.** As regras, no pertinente a obrigações e penalidades, devem ser graduadas de acordo com o porte da empresa (não apenas faturamento ou número de colaboradores), mas o grau de exposição que ela pode gerar para titulares de dados em razão da volumetria e características dos dados que trata. **Partimos nosso racional e premissa, a partir de exemplo de dois tipos de leis que enrijeceram o tratamento e que melhoraram a vida das pessoas no Brasil.** **Os exemplos abaixo são de leis com certo grau de severidade e que não implicaram no fechamento de empresas ou postos de trabalho:** 1. **Novo Código de Trânsito:** trouxe obrigações de usar cinto de segurança, cadeirinha para crianças no banco traseiro, proibição de transporte de pessoas em caçamba, novas regras para fixação de limites de velocidade, rigidez com embriaguez ao volante, sendo o descumprimento da lei, sancionado com: 1.1. novas regras inserindo a pontuação de infrações em CNH; 1.2. penalidades de suspensão do direito de dirigir para quem atinge o nível indicado de pontuação; 1.3. multas efetivas; **Resultado**: ainda longe do desejável, porém tem educado o brasileiro no trânsito, a ponto de reduzir drasticamente o número de mortes no trânsito em relação ao que vivenciávamos na década de 90;

	2. **Lei do rodízio de trânsito**: cidade de grande volume de tráfego de veículos e com poluição em níveis alarmantes, São Paulo estabeleceu o rodízio de veículos como regra. 2.1. Sujeição de todos os veículos, independentemente de serem da cidade de São Paulo, de uso particular ou corporativo; 2.2. Criação de exceções para situações que efetivamente precisam ser tratadas como tal, caso de veículos a serviço da saúde, de transporte de produtos perecíveis; 2.3. A limitação do uso de veículos foi realidade que impactou todo tipo de empresa, grande, média, pequena, profissionais liberais, que tiveram que se adaptar à nova realidade. 2.4. Multas por descumprimento com fiscalização eficiente e perda de pontos na CNH; **Resultado:** observância pela maioria da população, melhoria das condições de tráfego, ainda que não seja o desejável, dado ao volume de veículos e pessoas em transporte na cidade, melhora das condições do ar, com diminuição da poluição; **3. Leis ambientais:** O Brasil conta com leis de proteção ao meio ambiente que são severas, aplicam-se a todos, sem distinção. As dimensões do nosso território são desafios para identificação e punição de transgressores que praticam desmatamento de florestas, por exemplo. Entretanto, no campo das atividades negociais, o licenciamento de empresas e atividades que gerem impacto ao meio ambiente possuem rigoroso controle, inclusive com grande dificuldade de obtenção da licença. Durante o exercício da atividade licenciada, a fiscalização é rigorosa pelo Poder Executivo, Ministério Público, Associações de Proteção, dentre outras. 3.1. As novas práticas de mercado e a conscientização sobre sustentabilidade e consumo consciente foram determinantes para diminuição do número de empresas poluidoras ou que não tinham cuidado com o tratamento dos seus efluentes; 3.2. A conscientização desenvolvida a partir de políticas públicas, selos de responsabilidade ambiental para empresas e municípios, outorgados por entidades da sociedade, contribuíram para a difusão e multiplicação do conceito de empresas e cidades amigas do meio ambiente;

	3.3. As empresas que possuem esse reconhecimento têm obtido do mercado reconhecimento aos seus esforços e isso tem sido convertido e melhoria de resultados; **RESULTADO:** A solução em todas as questões Em que pese ainda haver muito por fazer, as leis ambientais promulgadas nas últimas décadas, o esforço dos órgãos de controle e fiscalização, têm contribuído para a busca de um ambiente mais sadio e de preservação do nosso ecossistema. Os exemplos acima, como dito, são de leis que foram aplicadas nas últimas décadas no Brasil e que melhoraram o ambiente social e negocial e que não apesar da severidade de suas medidas, não implicaram, de per si, em fechamento de empresas ou postos de trabalho. **Abaixo, exemplo de lei de importância indiscutível no ordenamento jurídico e que é responsável por uma nova cultura empresarial após seu advento, e que implicou no fechamento de empresas e postos de trabalho:** **Muito citada quando se fala da LGPD, tivemos na década de 90 o advento de lei que foi fator determinante para o desenvolvimento do mercado brasileiro e para que empresários e profissionais não capacitados e que desprezavam o respeito pelos direitos das pessoas com que se relacionam, quebrassem ou encerrassem suas atividades, esse o caso do:** 1. **Código de Defesa do Consumidor:** sua vigência trouxe uma série de inovações e que foi aplicada indistintamente a pequenas e grandes empresas, intermediadores e fornecedores, profissionais liberais, enfim, sua busca foi pela garantia de um mercado que fosse respeitado pelo consumidor por entender que ao realizar sua compra de bens ou aquisição de serviços estaria respaldado por: 1.1. Direito de garantia do produto; 1.2. Abatimento de preço para produtos com vícios ou sua substituição por um novo; 1.3. Obrigatoriedade de manutenção de peças de reposição por prazo de 5 anos; 1.4. Direito a indenização; 1.5. Direito de ter o ônus da prova invertido para que não fosse dizimado em disputas judiciais dada a disparidade de armas;

	1.6. **Direito de acesso a dados que são tratados pela empresa fornecedora de produtos e serviços, conforme seu artigo 43.** 1.7. **Diante do disposto no artigo 43, que se aplica a toda categoria de fornecedor, pequeno, médio ou grande, implicará em um diálogo de fontes e a minimização da LGPD para pequenas empresas, microempreendedores e profissionais liberais, não os afastará da obrigação de tratar o titular dos dados e seus direitos de forma semelhante a preconizada na LGPD.** **Prática diferenciada:** O CDC investiu muito na difusão da cultura da proteção dos direitos do consumidor e das obrigações a serem cumpridas pelos fornecedores, campanhas midiáticas, obrigatoriedade do exemplar da lei em local visível nas lojas físicas para o consumidor poder fazer valer o seu direito, criação de instâncias administrativas para solução de situações de menor potencial. **RESULTADO:** O CDC é norma referência mundial em matéria de proteção do consumidor e do mercado local, tem aplicabilidade de forma absolutamente padronizada no Brasil, trata de forma desigual aqueles que possuem disparidade de forças, mas apenas no ambiente das provas, não afasta da sua aplicação, muito mais severas que as preconizadas na LGPD, empresas em razão do seu porte. Há hoje um ambiente de segurança na aquisição de produtos certificados por entidades de controle como INMETRO, IPEM, dentre outros, há confiança nas instituições que defendem a aplicabilidade do CDC, como é o caso do PROCON, a segurança jurídica quanto as obrigações que devem ser cumpridas pelas empresas e quanto aos direitos que os consumidores têm. A partir das premissas fixadas acima, onde destacamos que a intervenção do legislador no ambiente social, se faz necessária muitas vezes inclusive para eliminar agentes nocivos, e que como resultado traz a melhoria, a profissionalização e a confiança no ambiente que sofreu a intervenção, nossa sugestão, bastante objetiva e racional, é assim pontuada: 1. Aplicação da lei a todo tipo de empresa e profissional pessoa física que trate dados com fins comerciais;

	2. Regulação administrativa pela ANPD de programa de conscientização nacional do cidadão e das empresas sobre direitos e deveres; 3. Profissionalização e regulação das empresas que atuam como Consultorias em Proteção de Dados, visando garantir ambiente regulatório respeitado pela sociedade 4. Criação de guias online e direcionamento pela ANPD, sobre o mínimo desejável em termos de proteção de dados, segurança da informação e boas práticas para micro empresas, MEI´s e profissionais liberais; 5. Garantia da segurança jurídica de que micro empresas, MEI´s e profissionais liberais, serão fiscalizados, avaliados e julgados baseadas nessas premissas minimamente essenciais em proteção de dados, segurança da informação e boas práticas; 6. Criação de certificação ou selo, para micro empresas, MEI´s e profissionais liberais, que voluntariamente e a cada período a ser definido pela ANPD, comprovem perante a autoridade a adoção dos padrões mínimos tratados no item anterior; 7. Criação de canal da ANPD para que micro empresas, MEI´s e profissionais liberais, possam sanar dúvidas na aplicabilidade da lei em situações concretas; 8. Certificar consultorias que apresentem programas de conformidade à lei para micro empresas, MEI´s e profissionais liberais, que atendam a requisitos fixados pela LGPD e regulados pela autoridade, como forma de criar diferencial competitivo para micro empresas, MEI´s e profissionais liberais de forma profissional; 9. Regular e tornar público, acessível para garantir respeito e segurança jurídica sobre os critérios que serão utilizados para avaliar a conduta em proteção de dados de todas as empresas, mas sobretudo de micro empresas, MEI´s e profissionais liberais; 10. Tornar público e objetivo o racional de sujeição e dosimetria das penas para todas as empresas, categorizando por porte ou tipo de exposição, se o caso; 11. Regular o *enforcement* ou seja, o dever dos parceiros comerciais de exigir da sua cadeia de relacionamentos, no que pertine a micro empresas, MEI´s e profissionais liberais, deixando claro o que pode e/ou deve ser comprovado em termos de cumprimento das obrigações regulatórias, para evitar que estas últimas sofram suspensões de contratos, por exemplo, dado representar elo de vulnerabilidade da empresa parceira; 12. Criar manual e aplicações online para observância das regras de *Privacy by design* e *Privacy by default*, específicos para micro empresas, MEI´s e profissionais liberais, afim de estabelecer a cultura de prevenção em proteção de dados;

Quais são as oportunidades relacionadas ao tema?	A regulação da proteção de dados e sua aplicabilidade não se tratam de oportunidade, mas de obrigação para sobrevivência do mercado brasileiro na concorrência com outros mais maduros e detentores de respeitabilidade em decorrência da clareza, rigidez e segurança jurídica em uma economia global, conectada, sobre como trata dados das pessoas com quem se relacionam.
Quais são as experiências internacionais sobre o tema?	A regulação da proteção de dados é tema recente na grande maioria dos países, de modo que em recente Congresso Internacional que realizamos na Universidade de São Paulo, Faculdade de Direito de Ribeirão Preto, em 2019, onde tratamos das preocupações com as regulações pela Autoridade Nacional de Proteção de Dados, a partir da perspectiva do que ocorria em outros países do globo terrestre, ficou claro que temos um sistema muito mais complexo que a grande maioria dos países, dificuldades decorrentes de diversidade de culturas regionais, diversidade de interpretação jurídica nos diversos estados da Federação, de modo que concluímos pela necessidade de uma solução que parta da nossa realidade, especialmente no pertinente à proteção de dados, segurança da informação e boas práticas de microempresas, MEI´s e profissionais liberais, caso contrário estaremos sujeitos a impingir regras não aderentes a essa realidade particular do Brasil.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Nessa ordem de prioridade: 1. Volume de dados pessoais tratados; 2. Grau de exposição para o titular que os tipos de dados pessoais tratados podem gerar; 3. Nicho de atuação: saúde, tecnologia, educação e varejo, possuem alta exposição. 4. Ambiente de atuação (físico ou digital); 5. Faturamento anual 6. Tempo de atividade empresarial 7. Número de colaboradores com acesso a dispositivos de informática
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)?	1. De acordo com a entrevista realizada com líderes de pequenas organizações europeias em 2019 pela GDPR.EU[5], plataforma online operada pela Proton Technologies AG, o cenário encontrado após um ano de vigência da *General Data Protection Regulation* é bastante desafiador. 2. Nesta pesquisa, foram entrevistados 716 líderes de pequenas empresas da Espanha, Reino Unido, França e Irlanda. Segundo apurado, notou-se, de forma geral, um

[5] GDPR Small Business Survey, 2019. Disponível em: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf. Acesso em: 08 fev. 2021.

	considerável desejo dessas pequenas companhias estarem aderentes à legislação de proteção de dados, fato que pode ser confirmado pelos altos investimentos realizados até o momento com consultorias especializadas e soluções de tecnologia da informação, estimando custos entre € 1.000 e € 50.000. 3. A maior parte dos líderes ainda entenderam que a conformidade com a proteção de dados não afeta o crescimento econômico de suas empresas, pelo contrário, é uma prática necessária não somente para torná-los competitivos no mercado, mas também para garantir a proteção dos seus próprios dados, uma vez que, em algum momento, se encontrarão na posição de titulares de dados. Assim, de modo geral, considera-se alto o nível de conscientização por parte das pequenas organizações na Europa, muito diferente do que se encontrará no Brasil com a LGPD. A atuação da União Europeia, através das Autoridades Nacionais de cada país-membro, foi imprescindível para criar essa cultura dentro das pequenas organizações. 4. A ICO (*Information Commissioner's Office*), Autoridade de Proteção de Dados do Reino Unido, tem se dedicado a auxiliar as pequenas organizações em sua conformidade com a *GDPR*, destinando, para tanto, uma central de recursos com dicas para iniciantes, *templates*, materiais, guias, comunicados, testes, cartilhas e demais conteúdos voltados para as necessidades específicas desse público, e que podem ser acessados e encontrados facilmente no site da organização (https://ico.org.uk/). Como uma dessas medidas de atuação voltadas para os agentes de pequeno porte, a ICO disponibiliza em seu site uma lista de verificação de autoavaliação com perguntas direcionadas para proprietários de pequenas empresas ou empresários individuais entenderem o seu negócio do ponto de vista da privacidade e proteção de dados. Concluída a lista de verificação, a ICO sugere ações práticas e orientações específicas, conforme resultado do teste. 5. Além disso, a ICO também disponibiliza modelos de cláusulas contratuais para pequenos comerciantes através de uma ferramenta interativa que os auxiliam a gerar

	automaticamente cláusulas que visam permitir a transferência internacional de dados para fora da União Europeia dentro dos regramentos da *GDPR*. [6] 6. Ainda assim, de acordo com o apurado na pesquisa da GDPR.EU, os líderes dessas pequenas organizações ainda não possuem conhecimento sobre conceitos básicos de segurança de dados, como o de criptografia de ponta-ponta. Isso ficou bastante evidente quando foi perguntado para os líderes por qual ferramenta era possível fazer uso dessa técnica de segurança, mas apenas 9% dos entrevistados citaram alguma válida como "VPN", "Mailchimp" e "Dropbox". As demais respostas não correspondiam a ferramentas que efetivamente realizam esse tipo de medida de segurança. 7. De acordo com o definido pela União Europeia no art. 30 da *GDPR*, empresas com mais de 250 funcionários são obrigadas a manter registros de suas atividades de processamento de dados. Já as empresas com menos de 250 funcionários, a manutenção de registros só será obrigatória se a organização realizar tratamento de dados regularmente, manipular informações confidenciais ou processar dados que possam ameaçar a violação de direitos dos titulares. Esse critério quantitativo é uma forma válida para não onerar agentes de pequeno porte que não fazem do processamento de dados sua principal atividade.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	1. A manutenção do registro de operações de tratamento de dados é uma atividade que, quando feita manualmente, requer grande dispêndio de tempo e zelo por parte do agente de tratamento. É certo também que as pequenas organizações não poderão comprometer parte da sua receita para contratar um funcionário destinado especificamente para essa função e nem mesmo conseguirão capacitar um funcionário dentro do seu quadro atual para realizar todos os registros necessários. 2. Aliado a tais dificuldades, está a contratação de ferramentas ou plataformas que fazem esses registros, classificações e fluxos de informações pessoais em conformidade com a

[6] https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/

	legislação, já que essas soluções de tecnologia são consideradas caras para o negócio, o requer um investimento fora da realidade dessas pequenas organizações. 3. Os impactos, portanto, seriam justamente no fluxo de caixa dessas empresas, pois não haveria soluções de baixo custo para torná-los, no atual momento, em conformidade com as regras de manutenção de registros da LGPD. Isso só seria possível se tais exigências fossem mais brandas e dentro de uma sistemática que facilitasse a execução e compreendesse a realidade de cada agente.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	A existência desse profissional na empresa traz mais benefícios do que o contrário. Sugerimos que não seja obrigatório, mas que seja considerada uma boa prática desejável, haja vista que a empresa não precisa ter funcionário dedicado para tanto, mas pode dispor de consultorias estruturadas para exercer essa função e colaborar com o programa de privacidade, manutenção da conformidade, monitoramento da sua aplicabilidade. Existem no Brasil consultorias que possuem projetos específicos para agentes de pequeno porte, como é o caso da LGPD Fácil, que atua por meio de Centro de Serviços compartilhados (CSC), onde uma equipe multidisciplinar com conhecimentos avançados em infraestrutura de TI, jurídico/regulatório, Segurança da informação e controle de processos, atuam como encarregado de proteção de dados, atendendo e monitorando digitalmente, com SLA´s definidos contratualmente, base de conhecimento experimentada, confidencialidade, e com custos adequados para esse tipo e porte de empresa.
Quais são os impactos da elaboração do relatório de impacto à proteção de	1. Nem todo agente de pequeno porte tem conhecimento ou mão de obra suficiente e capacitada para desenvolver um Relatório de Impacto à Proteção de Dados na forma

dados pessoais aos agentes de pequeno porte?	com que é requisitado pela LGPD, ou seja, com a obrigação de estabelecer uma matriz de riscos com medidas para mitigação e de verificar se há realmente uma violação de direitos fundamentais ou liberdades dos titulares, pois se trata claramente de um documento que requer conhecimentos técnicos e precisam ser produzidos e avaliados por alguém que saiba interpretar a legislação, conheça normas de *compliance*, normas ISO e Segurança da Informação, bem como tecnologia. 2. Dessa forma, a inobservância dos requisitos que devem ser preenchidos no relatório provavelmente impactará na ineficácia dessa ferramenta para agentes de pequeno porte. A elaboração do documento não terá valor se não estiver estruturado de forma que a ANPD ou outra autoridade seja capaz de identificar medidas efetivas para diminuir os riscos e perceber a eventual violação de direitos por esse Controlador. 3. No formato atual, o seu preenchimento pode inviabilizar o negócio do agente de pequeno porte, dada a tecnicidade, falta de conhecimento e o tempo dispendido já levantados. A sugestão, considerando a importância dessas pequenas companhias incluírem a privacidade desde o início de suas atividades, em obediência ao *privacy by design*, é definir requisitos mais flexíveis e pontuais que os encontrados atualmente na LGPD, mas, ao mesmo tempo, mais direcionado a realidade desse grupo. 4. Em grandes empresas, é essencial que se tenha conhecimento sobre o fluxo de processos no tratamento de dados, que muitas vezes é complexo e dependente de outras áreas da organização ou até de terceiros para seu correto preenchimento. Já em empresas menores, com menos processos, isso poderá ser mais facilmente resumido ou entendido de forma preliminar por meio de questionamentos prévios, capazes de mapear o perfil da empresa dentro dos regramentos da LGPD.

	5. A Autoridade Nacional de Proteção de Dados (ANPD) deverá levar em consideração também o papel dessas pequenas organizações no cenário brasileiro atual para o desenvolvimento da economia. As grandes companhias se relacionam com uma gama diversificada de agentes de pequeno porte, que orbitam, de forma satélite, nesses vultuosos negócios. Assim, é inegável que, dada as relações comerciais rotineiras entre grandes e pequenos, há uma dependência não só econômica, mas do ponto de vista da privacidade e proteção de dados, uma vez que não basta apenas as grandes companhias preencherem o Relatório de Impacto à Proteção de Dados e o demais requisitos legais, se os agentes de pequeno porte não tiverem em conformidade com essa obrigação ou, nos casos de apoio requerido, não tiverem capacidade para auxiliar no preenchimento desses relatórios, comunicar um incidente ou até mesmo mapear riscos de uma determinada operação. 6. Assim, sob pena de expor não só os dados pessoais que trata, mas também atingir, direta ou indiretamente, as grandes empresas nas quais se relaciona e cuja volumetria de informações é bem maior, os agentes de pequeno porte devem ser orientados para elaboração desses relatórios, ainda que em modelos alternativos. Assim, sugerimos, com base nas boas práticas fomentadas na União Europeia pela *GDPR,* as possibilidades para implementação do Relatório para tais agentes: a) Estabelecer uma cadeia de responsabilidades para cada organização; b) A revisão e/ou avaliação final realizada por pessoa capacitada para essa atividade, seja internamente ou externamente; c) Se externamente, possibilitar a contratação de ferramentas e/ou soluções, desde que devidamente certificadas para execução dessa tarefa;

	d) Possibilitar que o documento seja retificado, corrigido e complementado, ainda que mediante a critérios rígidos, assim como ocorre com o Imposto de Renda; e) Fornecer *templates* simplificados*,* guias, testes de verificação e/ou modelos pré-preenchidos para auxiliar no preenchimento, assim como ocorre no Reino Unido através da *ICO*; 7. Dentro dessa realidade em que há grande compartilhamento de dados entre grandes e pequenos negócios, extinguir o relatório poderá impactar negativamente para criação de uma cultura de proteção de dados no Brasil, uma vez que uma das funções do relatório é justamente documentar um procedimento delicado e sensível envolvendo informações pessoais, e que serve tanto para registro da operação, quanto para demonstrar o grau de zelo da empresa no processamento de dados. Além disso, também visa atribuir medidas preventivas, mapear e diminuir riscos e, ao final, evitar a violação de direitos e liberdades fundamentais.
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?	1. A quantidade de dados sensíveis e de crianças e adolescentes dependem muito mais do negócio da empresa do que o seu tamanho. Uma escola infantil ou pequeno consultório médico certamente processam mais dados pessoais sensíveis e de crianças do que uma grande empresa varejista, por exemplo. 2. Desse modo, cabe a Autoridade distinguir a natureza da atividade negocial de cada agente, por consequência, identificar qual está mais sujeita ao tratamento de dados pessoais sensíveis e de crianças e adolescentes, que merecem proteção especial da LGPD, direcionando as orientações e recomendações para adequar a sensibilidade percebida em consonância com a proporção tratada por cada instituição e não necessariamente pelo tamanho da organização;

Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	1. Implementar um programa de governança de dados, da forma em que foi estabelecido pela LGPD, poderá causar impacto negativo nas finanças dos agentes de pequeno porte e até inviabilizar seu negócio, a depender do porte da organização. 2. Ainda assim, a sua ausência total de um programa de governança de dados traria uma grande desconformidade com a LGPD, pois impactaria diretamente na falta de estrutura destinada a solucionar conflitos relacionadas aos dados, seja do ponto de vista da segurança da informação ou da própria LGPD. Ao mesmo tempo que, implementar um programa completo também não seria possível, pois não há como exigir, ao menos por enquanto, que uma pequena organização possa custear todas as ferramentas, treinamentos, capacitações, sem nenhum apoio externo. 3. Assim, uma sugestão seria adequar o programa de governança de dados ao porte, estrutura da operação, número de colaboradores, volumetria de dados pessoais tratados e grau de exposição a riscos para cidadão e a própria empresa. A fim de viabilizar esse procedimento, é possível atribuir a parceiros de negócio de médio e grande porte, que tenham a obrigação de cumprir com a LGPD e manter um programa de governança ativo, robusto e completo, a depender do tipo de relação e eventual vinculação dessas organizações ao serviço ou produto utilizado do agente de pequeno porte, de fornecer os mecanismos de governança e atribuir diretrizes quanto a obediência à Lei Geral de Proteção de Dados.

	4. A título de exemplo, isso poderia ocorrer de forma semelhante ao que ocorre nos contratos de franquia – entre master franqueador e franqueados – em que o Franqueador (agente de médio e grande porte), adaptável para o formato da proteção de dados, seria o responsável: a) por estabelecer um programa de governança de dados com implementação de boas práticas de segurança da informação e obediência as normas ISO b) disponibilizar o seu Encarregado de Proteção de Dados (DPO) para atender as franqueadas quando necessário; c) realizar treinamentos e capacitações dos colaboradores das franqueadas, ensinando o know-know relativo à privacidade, proteção de dados e segurança da informação; d) criar código de conduta, política de privacidade, política de cookies, em formato único para as franqueadas; e) estabelecer auditorias periódicas nos processos de tratamento de dados das franqueadas;
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	Em relação a implantação da Política de Segurança relativa a proteção de daods, os prováveis impactos são: a) Mudança de cultura, de modo que os pequenos agentes possam estruturar uma Política de Segurança da Informação e passe a olhar para seus procedimentos internos com viés da segurança virtual da mesma forma que ocorre na vigilância de espaços físicos; b) Tornar os comportamentos nas relações de processamento de dados mais previsíveis; c) Introduzir a segurança para as informações, tornando os procedimentos mais claros e transparentes para o titular dos dados

	d) viabilizar negócios com agentes e clientes de grande porte, que necessitam de um ambiente de proteção de dados estruturado e evidenciado.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	1. Ainda que essencial a avaliação sistemática de riscos para identificar vulnerabilidades e diminuir o risco de incidentes de violação e falhas de segurança da informação, não é comum que agentes de pequeno porte utilizem ferramentas ou métodos de avaliação de riscos de uma forma geral, ou seja, sequer há uma metodologia pré-definida para atribuir riscos gerais do seu negócio. Assim, exigir a implantação de um sistema de riscos específicos para a proteção de dados poderá causar estranhamento aos pequenos comerciantes, que não estão acostumados a esse tipo de avaliação dentro da sua empresa, salvo exceções. 2. Por outro lado, estabelecer parâmetros bem definidos sobre os possíveis riscos que essas organizações correm com a vigência da LGPD pode ter um impacto positivo para a população de forma geral. Paralelamente, temos como exemplo a vigência do Código de Defesa do Consumidor, em que os pequenos comerciantes passaram a ser obrigados a observar os riscos que suas práticas comerciais dissonantes com aquele regramento poderiam lhe causar: multas, sanções, perda de reputação e competitividade; influenciar na preferência do consumidor.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	De forma imediata para quem não tem como objeto final a atividade de manuseio de dados seria inviável. Sugestão: ser exigível apenas das empresas que atuam ou tem como objeto e atividade-fim o manuseio de dados.
Qual instrumento regulatório poderia ser utilizado para promover e	1. Criação de certificação ou selo, para micro empresas, MEI´s e profissionais liberais, que voluntariamente e a cada período a ser definido pela ANPD, comprovem perante a autoridade a adoção dos padrões mínimos tratados no item anterior;

incentivar a inovação nos agentes de pequeno porte?	2. Profissionalização e regulação das empresas que atuam como Consultorias em Proteção de Dados, visando garantir ambiente regulatório respeitado pela sociedade; 3. Certificar consultorias que apresentem programas de conformidade à lei para micro empresas, MEI´s e profissionais liberais, que atendam a requisitos fixados pela LGPD e regulados pela autoridade, como forma de criar diferencial competitivo para micro empresas, MEI´s e profissionais liberais de forma profissional;
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

RES: Tomada de Subsídios 2/2021, até o dia 24 de março de 2021.

Lirian Soares [redacted]

qua 03/03/2021 11:22

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

1 anexo

contribuicoes_PME_280121 (2) ANPD.docx;

Prezados Senhores

Em atendimento à tomada de subsídios 1/2021,dessa autoridade, iniciada no dia 29 de janeiro de 2021, segue minha contribuição sobre a regulamentação para microempresas e empresas de pequeno porte para ANPD - Lei Geral de Proteção de Dados Pessoais.

Com o intuito de colaborar, estamos à disposição.

Atenciosamente

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Dra. Lirian Cavalhero – Federação Nacional de Hotéis, Restaurantes, Bares e Similares

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (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 garantia de segurança,

boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais são os desafios/problemas regulatórios relacionados ao tema?	**As empresas de pequeno e médio porte terão que seguir processos padronizados pela ANPD, senão não terão condições financeiras e humanas para implantação da lei nas empresas.**
Existem sugestões para endereçamento do problema?	**Criar procedimentos básicos padrões para implantação da LGPD**
Quais são as oportunidades relacionadas ao tema?	**Com sistema padronizada, as empresas cumprirão a lei, e a implantação da lei deixa de ser um custo e passa a ser um diferencial.**
Quais são as experiências internacionais sobre o tema?	**Talvez o melhor modelo a ser implantado para as empresas de pequeno e médio porte são os da CCPA (California Consumer Privacy Act), nessa lei uma empresa tem que atender um dos seguintes pontos para se enquadrarem na lei: ter US$ 25 milhões ou mais em receita anual; ou possuir os dados pessoais de mais de 50.000 "consumidores, famílias ou dispositivos" ou ganhe mais da metade de sua receita anual vendendo dados pessoais dos consumidores.**

	Poderiam ser usados um desses limitadores em relação às micro e pequenas empresas, pois elas têm proteção constitucional, o que se justificaria.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	**O primeiro ponto e principal é a não necessidade do Encarregado, pois é um custo muito alto, e não há profissionais suficientes no país para suprir a demanda, podendo o sistema de comunicação funcionar por um SAC por telefone, programas de mensagens por celular ou e-mail.**
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)?	Há casos de empresas que saíram da UE ou simplesmente fecharam, porque não podiam arcar com os custos exigidos para cumprir a GDPR. As condições especiais para empresas com menos de 250 empregados, poderiam ser objeto de regulamentação pela ANPD, visando a aplicação da lei e a manutenção das empresas. Para essas empresas requisitos mínimos para implantação, por exemplo: inventário do tratamento, política de privacidade e de consentimento e um diagnóstico dos riscos.
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	**Impactos financeiros e de pessoal, por falta de pessoas qualificadas, por isso essa operação de tratamento precisa ser facilitada: forma de ingresso do dado, local de manutenção e tempo de retenção.**
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	**Essas empresas não terão como nomear encarregados, pelo custo e pela falta de mão de obra,**
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	**Acredito que esse deve ser um dos documentos necessários somente para demonstrar a forma simplificada, mas correta de tratar os dados**
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?	**No que tange dados sensíveis, realmente as empresas de pequeno porte precisarão se enquadrar a lei, pois seriam uma exceção à regra.**
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	**Se houver padronização e simplificação, esse impacto será reduzido, e poderá deixar de ser custo e passar a ser um diferencial.**

Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	**Esse é um dos documentos básicos que essas empresas precisam manter.**
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	**Essa avaliação não pode ser sistemática, salvo no caso de mudança comprovada na forma de tratamento do dado.**
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	**Esse dispositivo será ineficaz, pois as empresas não terão como fazer isso, e não trará nenhum benefício para o usuário**
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	**Padronização e simplificação**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	