Curitiba, 19 de fevereiro de 2021.

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

REF: Contribuições referente à tomada de subsídios nº 1/2021

Considerando que:

i) Pelo preceito constitucional do art. 133, reproduzido no art. 2º do Estatuto da Advocacia (Lei nº 8.906/94), o Advogado é indispensável à administração da Justiça;

ii) A Ordem dos Advogados do Brasil tem por missão institucional o zelar pela defesa da Constituição, da ordem jurídica do Estado Democrático de Direito, da justiça social, e pugnar pela boa aplicação das leis e pelo aperfeiçoamento da cultura e das instituições jurídicas; conforme art. 44, I, da Lei nº 8.906/94;

iii) As mudanças na dinâmica social – especialmente aquelas ligadas à livre iniciativa de microempresas e empresas de pequeno porte, constituídas na forma prevista Lei Complementar nº 123, de 14 de dezembro de 2006, e sua interface com os direitos e garantias fundamentais do indivíduo, tal como elencadas na Constituição da República e normas infraconstitucionais que delimitam seu alcance – exigem a inovação na regulamentação das relações entre os indivíduos, especialmente na atuação do advogado em defesa dos direitos do cidadão e da livre iniciativa, conforme Resolução n. 02/2015, da Ordem dos Advogados do Brasil;

iv) A Ordem dos Advogados do Brasil Seccional Paraná, por sua Comissão de Gestão e Inovação, reuniu membros com atuação profissional e acadêmica voltada à área de Privacidade e Proteção de Dados;

A Ordem dos Advogados do Brasil - Seccional Paraná, ciente da consulta pública para tomada de subsídios nº 1/2021, lançada pela Autoridade Nacional de Proteção de Dados (ANPD), vem, por meio do presente expediente, **REGISTRAR** suas contribuições para o aprimoramento do sistema normativo-regulatório no contexto do objeto da consulta proposta pela ANPD.

Cássio Lisandro Telles
Assinado de forma digital por Cássio Lisandro Telles
Dados: 2021.02.19 16:00:36 -03'00'

CASSIO LISANDRO TELLES – OAB/PR 15.225
Presidente da Ordem dos Advogados do Brasil - Seccional Paraná

Relatores:

Rhodrigo Deda Gomes
Assinado de forma digital por Rhodrigo Deda Gomes
Dados: 2021.02.19 11:22:57 -03'00'

RHODRIGO DEDA GOMES – OAB/PR 55.220
Presidente da Comissão de Inovação e Gestão da OAB/PR

DANTON HILARIO ZANETTI DE OLIVEIRA
Assinado de forma digital por DANTON HILARIO ZANETTI DE OLIVEIRA
Dados: 2021.02.19 10:55:15 -03'00'

DÂNTON HILÁRIO ZANETTI DE OLIVEIRA – OAB/PR 58.323
Coordenador do Grupo Permanente de Discussão sobre Privacidade e Proteção de Dados da OAB/PR

Membros integrantes do grupo de trabalho:

Albadilo Silva Carvalho – OAB/PR 44.016

Anne Carolina S. Amador Kozikoski – OAB/PR 32.064

Cinthia Obladen de Almendra Freitas – Membro Consultivo

Eduarda Francine P. de Santana – OAB/PR 98.997

Evelyn Moreno Weck – OAB/PR 42.944

João Guilherme Duda – OAB/PR 42.473

Joelson Ribas Osti – OAB/PR 80.231

Julio Herman Faria – OAB/PR 98.131

Rafael Almeida Oliveira Reis – OAB/PR 90.642

Rafaela Vialle Strobel Dantas – OAB/PR 33.244

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

NOME DA INSTITUIÇÃO: Comissão de Inovação e Gestão da Ordem dos Advogados do Brasil – Seccional do Paraná

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 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 EM RESPOSTA À TOMADA DE SUBSÍDIOS

Por intermédio dos membros da Comissão de Inovação e Gestão, a Ordem dos Advogados do Brasil - Seccional Paraná, ciente da consulta pública para tomada de subsídios nº 1/2021, lançada pela Autoridade Nacional de Proteção de Dados (ANPD), vem, por meio do presente expediente, **REGISTRAR** suas contribuições para o aprimoramento do sistema normativo-regulatório no contexto do objeto da consulta proposta pela ANPD.

Quais são os desafios/problemas regulatórios relacionados ao tema?

Já em sua gênese, a Lei Geral de Proteção de Dados (LGPD) carrega consigo um aparente paradoxo: a difícil missão de conciliar a proteção de dados pessoais, direito fundamental e individual, e o desenvolvimento tecnológico e da inovação que, numa sociedade em rede[1] e num contexto econômico *data driven,* coloca tais interesses em polos opostos.

Quiçá, o maior desafio regulatório seja justamente encontrar caminhos viáveis para a flexibilização de obrigações legais impostas aos agentes de tratamento de dados pessoais, sem que isso signifique colocar em xeque os direitos fundamentais e garantias individuais, especialmente quando estas podem, potencialmente, gerar abalo frente a direitos da personalidade dos cidadãos e titulares de dados pessoais.

É sabido que o *General Data Protection Regulation* (GDPR), o regulamento europeu de proteção de dados pessoais, tanto em virtude do histórico intergeracional de leis e normas regulando ora nacional, ora comunitariamente o tema da privacidade e proteção de dados, quanto em razão dos conhecidos efeitos extraterritoriais projetados pelo regulamento em face de nações que não compõem o bloco econômico da União Europeia.

No entanto, é preciso considerar que o Brasil possui ainda não possui uma profunda cultura de proteção de dados, de modo que a reação de mercado à necessidade de adequação e implementação de medidas organizacionais capazes de demonstrar conformidade com a LGPD tem demonstrado que diversas das exigências legais dependem de um amadurecimento cultural, o que, certamente, não ocorre com a simples entrada em vigor de uma lei.

Desta feita, o papel da ANPD é fundamental para tornar factível o processo – contínuo – de aderência da comunidade empresária à LGPD, especialmente no que tange às Microempresas (MEs) e Empresas de Pequeno Porte (EPPs).

Não se pode olvidar que cabe à União, aos Estados, ao Distrito Federal e aos Municípios dispensarem às microempresas e às empresas de pequeno porte, assim definidas em lei, tratamento jurídico diferenciado, visando a incentivá-las pela simplificação de suas obrigações administrativas, tributárias, previdenciárias e creditícias, ou pela eliminação ou redução destas por meio de lei.

[1] CASTELLS, Manuel. **A Sociedade em Rede.** Trad. Roneide Venancio Majer, 21ª ed. São Paulo: Paz e Terra. 2020, p. 124.

Esse princípio constitucional foi consolidado pelo Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte – Lei Complementar n.º 123/2016, o qual também ressalta em seu artigo 1º, §3º, que toda nova obrigação que atinja as microempresas e empresas de pequeno porte deverá apresentar, no instrumento que a instituiu, especificação do tratamento diferenciado, simplificado e favorecido para cumprimento.[2]

Também a Lei Complementar nº 167/2019[3], introduziu o artigo 65-A e parágrafos, na referida Lei Complementar 123/2016, conceituando as startups como "empresas 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". E, ainda, conforme § 2º, as startups caracterizam-se por desenvolver suas inovações em condições de incerteza que requerem experimentos e validações constantes, inclusive mediante comercialização experimental provisória, antes de procederem à comercialização plena e à obtenção de receita.

Dentro de um contexto de marcos legais tão diferenciadores, surge a Lei nº 13.874, de 20.09.2019[4], concebida com a finalidade de que as atividades econômicas, quando diante de sujeição a regulamentos ou regulação, tenham suas particularidades avaliadas, segundo critérios que serão abordados no Tema nº 3 deste Documento, com vistas a minimizar o impacto que a edição de tais normas regulamentares possam acarretar ao livre desenvolvimento de tais atividades, em especial aquelas de menor porte, baixo risco ou as que possam inovar no mercado competitivo, melhorando a ambiência concorrencial.

Existem sugestões para endereçamento do problema?

Por brevidade, opta-se por endereçar o questionamento diretamente no corpo da minuta, quando das considerações elaboradas para cada um dos tópicos objeto da consulta lançada pela ANPD.

Quais são as oportunidades relacionadas ao tema

A estruturação e, sobretudo, atuação da ANPD era muito aguardada pela sociedade civil. A LGPD proporciona bastante campo para que a autoridade trabalhe lacunas regulatórias e, assim, estabeleça diálogo entre os beneficiários da norma (titulares) e aqueles que a ela estão sujeitos (agentes de tratamento *lato sensu*).

[2] PLANALTO. Lei Complementar nº 123, de 14 de dezembro de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm>. Acessado em 10 fev. de 2021.
[3] PLANALTO. Lei Complementar nº 167, de 24 de abril de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp167.htm>. Acessado em 10 fev. de 2021.
[4] PLANALTO. Lei nº 13.874, de 20 de setembro de 2019 (Declaração de Direitos da Liberdade Econômica). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm>. Acessado em 10 fev. de 2021.

Desta feita, as oportunidades, em suma, residem em permitir a aderência de uma norma que tem forte inspiração no ordenamento jurídico europeu, onde, como será detalhadamente abordado em tópico próprio, já possui longa trajeto civilizatório em relação à proteção de dados pessoais, o que não se pode simplesmente "replicar" através de uma "fórmula" legal. Há, portanto, que se permitir que a proteção de dados seja incentivada e facilitada para que esta nova *ratio* seja internalizada nos negócios brasileiros de forma bem sucedida.

Quais são as experiências internacionais sobre o tema?

Para entender o GDPR é necessário voltar um pouco no tempo. Apesar de entrar em vigor em 2016 (com vigência e produção de efeitos a partir de maio de 2018), a matéria é regulamentada há longa data dentro da União Europeia. O Parlamento e o Conselho Europeu fazem uso de Diretivas para exigir que os Estados-membros alcancem determinados resultados, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios[5]. Para que a Diretiva produza efeitos a nível nacional, os Estados-membros devem editar uma Lei com vistas a sua transposição. A transposição nacional é obrigatória e caso um país não a realize a Comissão poderá iniciar um processo por infração junto ao Tribunal de Justiça da União Europeia[6].

A Diretiva 95/46 foi a primeira a tratar sobre o direito a proteção de dados na União Europeia. Com 72 "considerandos" e 34 artigos[7], determinava que os Estados-membros editassem leis nacionais sobre a proteção de dados para assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais[8].

Referida Diretiva vigorou por mais de 20 anos quando foi revogada pelo GDPR, em razão das mudanças tecnológicas, uma vez que editada em um momento ainda incipiente da internet, e das diferenças entre as Leis sobre proteção de dados editadas nos Estados-membros.

Segundo o Considerando 9 do GDPR, os princípios da Diretiva continuam valendo, mas ela foi revogada pois não evitou a insegurança jurídica ou a opinião pública de que permanecem os riscos para a proteção de seus dados. [9]Ou seja, o

[5] Art. 288, Tratado Sobre o Funcionamento da União Europeia (TFUE).
[6] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527. Acesso em 06/02/2021
[7] A legislação europeia é conhecida por seus considerandos, que geralmente são em maior número do que os próprios artigos.
[8] Art. 1, Diretiva 1995/46.
[9] Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.

GPPR surge para trazer novos conceitos e adaptar a legislação às novas tecnologias, bem como para harmonizar a legislação sobre proteção de dados nos Estados-membros[10].

Micro Pequenas e Médias Empresas

De acordo com a definição da Comissão Europeia, dois são os parâmetros para essa classificação: (i) menos de 50 milhões de euros em receita e (ii) menos de 250 empregados contratados.

As ME e EPP são obrigadas a garantir aos seus sujeitos de dados os direitos básicos listados no GDPR do artigo 15º ao artigo 22; isso implica que as ME e EPP devem ter certeza de que existem sistemas e processos implementados para que esses direitos sejam cumpridos dentro do prazo legal estabelecido (um mês). Uma vez identificados o tipo de dados tratados, até mesmo as ME e EPP são obrigadas pelo GDPR a avaliar quais tipos de processamento de dados podem resultar em um alto risco para os indivíduos.

Apesar das evidentes dificuldades de conformidade das ME e EPP[11] , em relação aos grandes *players*, o Regulamento não comporta exceção à aplicação da lei, notadamente por estabelecer um vínculo entre risco e responsabilidade. Nesse contexto, indistintamente, considera-se irregular o tratamento de dados, por dois aspectos: *(i)* pela inobservância aos ditames da GDPR; e *(ii)* pelo não fornecimento da segurança adequada à atividade realizada[12].

A Diretiva não mencionava tratamento especial às micro empresas e empresas de pequeno porte, já o Regulamento prevê apenas algumas facilidades.

De fato, a concepção de que o Regulamento Europeu é aplicado a todas as organizações, independentemente da sua dimensão, porém, a depender da criticidade da atividade realizada, se confirma por meio da resposta à pergunta: “As regras se aplicam às PME?”, extraída do endereço eletrônico da Comissão Europeia[13]

> “Sim, a **aplicação do regulamento de proteção de dados não depende da dimensão da sua empresa / organização, mas da natureza das suas atividades.** Atividades que apresentam alto risco para os direitos e liberdades das pessoas, sejam elas realizadas por uma PME ou por uma grande corporação, desencadeiam a aplicação de regras mais rígidas. No entanto, algumas das obrigações do GDPR podem não se aplicar a todas as PMEs.
> Por exemplo, empresas com **menos de 250 funcionários não precisam manter registros** de suas atividades de processamento, a

[10] https://migalhas.uol.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia

[11] https://www.crowe.com/pt/insights/20200527-o-rgpd-e-as-pequenas-e-microempresas

[12] BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR**. – 1. ed. – São Paulo: Thomson Reuters Brasil, 2020

[13] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en. Acesso em 15/02/2021.

> 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 PMEs 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" (grifos no original).

Feitas estas considerações, passa-se a analisar alguns dos aspectos regulatórios previstos no GDPR que afetam diretamente as atividades de MEs e EPPs.

Código de Conduta

Em alguns casos, como na (a) elaboração de códigos de conduta (art. 40 e considerando 98), (b) na execução de competências da Comissão (considerando 167) e (c) na emissão de certificação permite a ponderação de medidas específicas, conforme suas necessidades.

Dispensa de registro de atividades

No Considerando 13 e no art. 30º é prevista uma derrogação para as organizações com menos de 250 funcionários relativamente à conservação do registro de atividades.

Ou seja, empresas com menos de 250 funcionários não têm que manter registros de suas atividades de processamento, a menos que o processamento de dados pessoais seja uma ocorrência/atividade regular, represente uma ameaça potencial aos direitos e liberdades dos indivíduos ou inclua dados confidenciais ou registros criminais.

Importante salientar que essa é a única hipótese do GDPR que fornece isenção com base em critério quantitativo.

Também é incentivado que as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controle, levem em consideração as necessidades específicas das ME e EPP no âmbito de aplicação do Regulamento.[14]

[14] Definição de PME conforme o artigo 2.º do anexo da Recomendação 2003/361/CE da Comissão.1. A categoria das micro, pequenas e médias empresas (PME) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros. 2. Na categoria das PME, uma pequena empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede 10 milhões de euros. 3. Na categoria das PME, uma microempresa é definida como uma empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.

Encarregado de proteção de dados

Em relação à nomeação do encarregado de proteção de dados, também chamado de DPO (sigla em inglês para Data Protection Officer), as ME e EPP seguem a mesma regra das demais, prevista no art. 37, 1, do GDPR.

No caso das ME e EPP , a hipótese principal em que seria obrigatória a designação do DPO está prevista no item "*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".*

Assim, as ME e EPP são obrigadas a nomear um Oficial de Proteção de Dados sempre que o processamento for seu principal negócio e se representar ameaças aos direitos e liberdades de um indivíduo.

Quando a atividade principal envolva operações de processamento em larga escala ou dados pessoais confidenciais, o GDPR sugere a nomeação de um DPO, uma figura independente da gestão e da equipe que realiza o processamento (mesmo que ele ou ela possa ser um membro do pessoal da empresa).

Multas

Em relação às multas, o GDPR prevê limites máximos de 20 milhões de euros ou 4% do volume de negócios global.

Porém, os valores das multas poderão variar conforme a legislação nacional. Na Lei portuguesa (Lei n. 59/2019), por exemplo, existem valores mínimos previstos[15]. Segundo o art. 52, em caso de infração grave a multa mínima é de 1000 euros e de infrações muito graves 2000 euros para as PME. A fixação do valor caberá à CNPD que tem em conta, entre outros critérios, o volume de negócios, o balanço anual e a dimensão (nº de trabalhadores e natureza dos serviços prestados) da empresa, assim como o caráter continuado da infração[16].

Casos

Algumas empresas brasileiras que tinham como estratégia a monetização de dados pessoais na União Europeia precisaram sair do ar às vésperas da entrada em vigor do GDPR, como Unroll.me, Klout, Drawbridge e o jogo Ragnarok[17].

[15]Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3123A0052&nid=3123&tabela=leis&pagina=1&ficha=1&so_miolo=?area=Identifica%E7%E3o%20civil%20e%20criminal&nversao=#artigo

[16] Disponível em: https://www.phcsoftware.com/business-at-speed/rgpd-portugal-multas/

[17] Disponível em: https://exame.com/pme/gdpr-nova-lei-europeia-de-dados-pessoais-ja-afeta-startups-brasileiras/

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

Ao analisar o texto da LGPD, extrai-se do espírito do legislador infraconstitucional uma noção comum de proporcionalidade entre os encargos que a lei impõe aos responsáveis por tratamentos de dados e, daí, seus contornos regulatórios. O tratamento diferenciado conforme "porte" empresarial tem raiz histórica e hierárquica constitucional, remontando à própria ideia de isonomia (art. 5º, *caput*, CRFB), segundo a máxima aristotélica, que no contexto das microempresas (MPs) e Empresas de Pequeno Porte (EPPs) inspira a concessão de tratamento diferenciado a tais agentes de mercado, em razão de suas capacidades técnicas e econômicas distintas. Essa diferenciação também encontra inspiração no direito comparado, em especial a partir do GDPR.

De outro lado, os dispositivos da LGPD que comungam dessa axiologia e teleologia que prega a necessidade de tratamento diferenciado em vistas a atenuação de obrigações legais, há três conceitos distintos relacionados a "porte" e mais um (art. 55-J, XVIII) relacionado à inovação. A questão do porte advém do artigo 179 e a da inovação do artigo 218, ambos da Constituição Federal.

Então, dentre outras, adota-se a premissa de que a questão não diz respeito apenas à delimitação do "porte" dos agentes, mas à definição de quais agentes merecem tratamento diferenciado em razão de porte e/ou atividades de inovação tecnológica.

Passa-se à análise individualizada dos três conceitos em questão.

Microempresas e empresas de pequeno porte.

Com a devida vênia, no caso deste conceito, presente no art. 55-J, XVIII, não há competência delegada do legislador para regulamento da ANPD. O porte relacionado ao conceito de empresa já está definido pela LC 123/2006 e, seja pelo princípio da legalidade, seja por coerência do ordenamento jurídico, não se deve admitir inovação por via regulamentar administrativa.

Assim, para fins do art. 55-J, XVIII, devem ser consideradas microempresas e empresas de pequeno porte aquelas que atenderem aos critérios da LC123/2006 ou outra lei (em sentido estrito) que estabeleça definição diversa e/ou excepcional. Ou seja, a competência da ANPD para delimitar quais sujeitos se beneficiam de tratamento diferenciado em razão de porte empresarial, atualmente orientado por faturamento, já se encontra vinculada por lei, sem margem de discricionariedade ou preenchimento de conceito indeterminado. Como paralelo normativo, tem-se que o GDPR adotou essa sistemática de diferenciação como critério geral, remetendo-se, em seu artigo 39, à recomendação 2003/361/CE, por sua vez "relativa à definição de micro, pequenas e médias empresas", com base em "volume de negócios", extraídos de critérios contábeis, tal qual ocorre na LC 123/2006.

“Porte da Entidade” e “Porte dos Responsáveis”

No art. 55-J, VIII, da LGPD, além de não haver referência expressa a um conceito já legalmente delimitado, tem-se o termo “porte” (aspecto subjetivo) acompanhado de referências às atividades que realiza (aspecto objetivo). Portanto, deduz-se que o tratamento diferenciado decorre não de atributos específicos do sujeito (como faturamento), mas também das atividades que realiza. Essa combinação visa a mitigar encargos regulatórios sobre atividades de menor complexidade e com menor volume de dados. Por exemplo, determinadas empresas, de faturamento intermediário, a depender do mercado que atuam, podem ter tratamentos de dados de volume e complexidade, interesse e significância módicos, enquanto outras, de faturamento aquém dos limites da LC 123/2006, podem ter atividades de tratamento bastante significativas e críticas do ponto de vista da proteção de dados pessoais.

Salvo melhor juízo, é possível afirmar que o tratamento diferenciado decorrente de aspectos subjetivos de “porte” deve ser considerado em face dos critérios já previstos na LC 123/2006. Do contrário, ao não conceder tratamento simplificado e micro e pequenas empresas, a ANPD teria que partir de hermenêutica da LGPD que colidiria com o disposto no art. 179 da Constituição. Não se pode olvidar que a LGPD, embora concretize princípios fundamentais de privacidade, orienta atividade econômico-regulatória da ANPD, cuja autoridade, em última ratio, advém do artigo 174 da Constituição Federal, devendo guardar coerência com todo o capítulo da Ordem Econômica da Constituição.

Todavia, o legislador (no caso, pela LGPD), não pode ser ignorado. É princípio hermenêutico que no texto legal não há conteúdos despidos de efeitos, meramente decorativos. Assim, salvo melhor juízo, entendemos que o art. 55-J, VIII amplia o benefício para além de micro e pequenas empresas, contemplando-se diferenciação também a partir das *atividades* de tratamento de dados em questão.

Neste caso, as métricas são mais variadas (número de titulares, espécies de dados, dimensão econômica relacionada), e dependem de critérios decorrentes da expertise da ANPD e que, seguramente, deverão ser periodicamente revistos, seja pela evolução das tecnologias, seja pela curva aprendizado regulatório.

Iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação.

Aqui há um especial interesse do legislador em favorecer, e em não prejudicar, um ambiente de inovações tecnológicas e empresariais, especialmente aquelas referidas no art. 65-A, da LC 123/2006. As atividades de inovação, notadamente em *startups*, são marcadas pela incerteza e por uma governança frequente imatura, mas em franco desenvolvimento, bem como pela dificuldade no cumprimento de obrigações legais, notadamente aquelas acessórias e “burocráticas”, que elevam seus custos de transação.

Assim, o tratamento diferenciado exige a "autodeclaração" da condição de *startup*, podendo a autoridade definir (quando editar "normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos") se isso será concedido por requerimento ou se bastará a inovação deste atributo subjetivo quando o agente já estiver submetido a alguma obrigação regulatória em concreto. A segunda opção afigura-se mais razoável, sob pena de se criar uma nova obrigação acessória às empresas inovadoras em questão: informar o quanto antes a ANPD que ela se entende como *startup*.

Por sua unilateralidade, a declaração constituiria presunção relativa da condição de *startup*, que pode ser afastada concretamente sempre que se verificar o descompasso com os ditames do art. 65-A, da LC 123/2006, ou qualquer tentativa deliberada de burla ao regime de proteção de dados previsto na LGPD. Ou seja, a empresa se declara *startup* ou iniciativa ligada à inovação, mas não realiza atividades empresariais de caráter "incremental" ou "disruptivo", inerentes à definição de *startup* ou empresa de inovação.

No momento da redação deste parecer, o ordenamento jurídico começa a receber as suas primeiras definições legais de *startup* e empresas de inovação. Além de tramitarem projetos de lei específicos na temática – que, caso promulgados, deverão ser observados pela autoridade regulatória no futuro – observamos que a LC 167/2019 alterou a LC 123/2006 justamente para incluir tais conceitos.

Nessa esteira, é importante ressaltar a identidade de redações da LGPD com a LC 123/2006, conforme se infere do art. 55-J, VIII, LGPD e do art. 65-A, LC 123/2006, quanto às *"iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação".* Portanto, o legislador ressalvou "para fins desta Lei", mas o conceito legado pela LC 123 não pode ser ignorado pela ANPD, salvo justificativa técnica específica à realidade de tratamento de dados.

Conclui-se, pois, que para os fins do art. 55-J, XVIII, deve ser integralmente observada a LC 123/2006 pela ANPD, especialmente no que tange a porte da empresa e, quanto à sua característica inovadora, pelo menos enquanto não promulgada lei federal, mais especial na temática.

De acordo com a LGPD, as regras são aplicáveis igualmente independentemente do tamanho da empresa.

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no

> momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

No entanto, o regramento reconhece, no art. 55-J, XVIII, a possibilidade de a ANPD criar procedimentos diferenciados para alguns negócios:

> (...) XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei.

Portanto as micro e pequenas empresas, empresas de pequeno porte, MEIs e empresas de inovação estão sujeitas à LGPD, mas podem ter atenuadas algumas exigências em razão das suas especificidades.

A LGPD vem sendo encarada como um desafio especialmente desafiador para essas pequenas empresas, que, por vezes, ostentam poucos recursos. A preocupação dos empresários gira em torno dos riscos que podem representar os novos custos, as sanções, a burocracia e a interferência nos negócios.

A discussão é importante porque as empresas de pequeno porte representam 99% de todas as empresas do Brasil e são responsáveis por quase 30% do PIB. Dificultar a sobrevivência desses negócios sufocaria o crescimento do país em um péssimo momento advindo da crise sanitária do Covid-19.

Países mais maduros na discussão sobre proteção de dados têm optado por uma aplicação diferenciada a esses negócios. Porém, o regramento europeu não tem necessariamente isenções a pequenas empresas. Na GDPR, as empresas consideradas de pequeno porte (com menos de 250 funcionários), são favorecidas em apenas dois aspectos: a menos que o processamento de dados seja uma atividade típica do empreendimento ou represente, de fato, uma ameaça potencial aos direitos e liberdade dos titulares, as empresas não são obrigadas a manter registro das atividades de tratamento. Em relação ao encarregado de dados, as pequenas empresas europeias só são obrigadas a nomear um profissional para a função se o processamento de dados for o negócio principal da empresa ou se o processamento apresentar, de fato, uma ameaça potencial aos direitos e liberdade dos titulares.

Ressalva-se que as atribuições do encarregado no GDPR são muito mais amplas e complexas do que as estipuladas pela lei brasileira ao mesmo profissional e acredita-se que, a partir das regulamentações posteriores, o encarregado assumirá responsabilidades mais complexas também no Brasil, exigindo-se das empresas a nomeação de um funcionário ou terceiro responsável por essas funções.

A nomeação de um encarregado preocupa as pequenas empresas, pois envolve a contratação de mais um funcionário ou designação de alguém capacitado dentro da empresa. Como o texto está hoje, o cumprimento é

perfeitamente adaptável a quase todos os tipos de empresas, inclusive às pequenas empresas, mas diante da ampliação das competências, as empresas precisarão contratar um profissional especializado ou capacitar os seus empregados, o que é de grande preocupação para os empreendimentos de pequeno porte.

De acordo com o artigo 39º do GDPR, as funções do DPO envolvem:

(a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante e os trabalhadores que tratem os dados, a respeito das suas obrigações e de outras disposições de proteção de dados;

(b) Controlar a conformidade com o regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes.

(c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização;

(d) Cooperar com a autoridade de controle;

(e) Ponto de contacto para a autoridade de controle sobre questões relacionadas com o tratamento.

Enquanto no Brasil, tais atividades consistem em:

> Art. 41., §2º:
>
> (...)
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
>
> (...)
>
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Verifica-se que a opção europeia em diferenciar o tratamento dispensando às pequenas empresas merece elogios porque considera o contexto em que as empresas estão inseridas.

Muitas vezes, apesar do número pequeno de funcionários, as empresas processam uma grande quantidade de dados e apresentam riscos a direitos e liberdade dos titulares (exigindo-se a e dedicação e um encarregado de dados por exemplo), mas, em outras, apesar de uma grande quantidade de funcionários, devido ao pequeno fluxo de dados de pessoas físicas, a mesma exigência de torna desnecessária.

Para determinar quais são os requisitos que devem ser flexibilizados em favor das pequenas empresas é preciso considerar as principais dificuldades que veem sendo enfrentadas em países mais maduros na questão e adaptar à realidade brasileira.

Alguns órgãos na Europa, como é o caso do CEPYME, revelaram que a principal dificuldade para essas empresas é a gestão de recursos humanos e econômicos.

Sem dúvida, no Brasil, não será diferente. Mas, em regra, deve haver a aplicação da norma a todos os empreendimentos, respeitando-se as suas características e possibilidades particulares.

Conclui-se que o maior desafio no âmbito da LGPD será a implementação prática da lei. As empresas, de todos os portes, terão que organizar a estrutura empresarial pensando no dado desde a sua chegada, na empresa, até sua saída. As múltiplas realidades empresariais terão que lidar com mais um desafio, que, fortuitamente, poderá se tornar um diferencial competitivo.

Para isso, é aconselhável que as empresas, de todos os portes, envidem esforços para garantir que seus empregados, equipes, prestadores de serviços e parceiros estejam a par da importância da adaptação dentro das pequenas empresas, sempre dentro das medidas razoáveis e adaptáveis ao negócio em questão.

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 acordo com o artigo 5º, VIII, da Lei nº 13.709, de 14.08.2018[18], a LGPD, o encarregado de dados é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Segundo o artigo 41 da Lei, o controlador deverá indicar o encarregado pelo tratamento de dados pessoais, que terá, segundo o seu §2º, as seguintes atividades: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Ainda, segundo o §3º, da Lei, a autoridade nacional poderá estabelecer normas complementares sobre a

[18] PLANALTO. Lei 13.709, de 14.08.2018 (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em 10 fev. de 2021.

definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Exatamente com fundamento neste último parágrafo é que se analisa as hipóteses cabíveis e justificáveis de dispensa da necessidade da indicação do encarregado de dados, considerando, principalmente que o escopo da Audiência Pública da ANPD visa a simplificação da regulamentação e a avaliação do impacto regulatório (AIR) relativas às empresas de pequeno porte e as startups, além de pessoas físicas que tratem dados pessoais, todos designados como agentes de tratamento de pequeno porte. Segundo Eduardo Pereira Maroso, o profissional encarregado de tais atribuições deverá um especialista com conhecimentos do regramento jurídico, técnicas de gestão de processos, bem como de tecnologia, de sorte a garantir que as boas práticas da empresa, bem como as suas regras (normas internas) estejam em *compliance*, além de facilidade de relacionamento, em vista a função de atender o titular e intermediar o relacionamento entre o controlador e a autoridade nacional, gerindo conflitos e interesses da melhor forma[19].

Percebe-se, um profissional – ou mesmo uma empresa de assessoria contratada, pois a LGPD permite que essa função seja de mercado, não necessariamente um colaborador da própria empresa – trará custos de contratação e manutenção.

Segundo levantamento da Confederação Nacional da Indústria (CNI)[20] o custo de contratação de um DPO (*Data Protection Officer*), ou Encarregado de Dados, entre nós, foi estimado em R$ 360.000,00, anuais, que equivale praticamente ao teto do faturamento das microempresas. Óbvio que este parâmetro pode ser entendido segundo realidades locais, os portes da empresa e as ofertas em mercado de trabalho para profissionais do ramo, e tais custos poderão ser inferiores, em pelo 50% do levantamento da CNI. Entretanto, para a maioria esmagadora de micro e pequenas empresas dispor de um Encarregado de Dados, como pretende a lei, dedicado às atividades – e sem conflito de interesses, por exemplo com a área comercial, segundo as melhores práticas de governança – é um sonho que não se adequa à realidade dos pequenos empreendimentos.

No país, atualmente, conforme levantamento disponibilizado pelo SEBRAE, existem aproximadamente 19.228.000 empresas, sendo que destas, 9.810.400 são MEI (51,02%), 6.586.490 são ME – Microempresas (34,25%)[21]. Logo, 85,27% das empresas regularizadas, no Brasil, possuem faturamento anual igual ou inferior ao custo de manutenção de um Encarregado de Dados.

---

[19] MAROSO, Eduardo Pereira *in*: LGPD – LEI GERAL DE PROTEÇÃO DE DADOS: SUA EMPRESA ESTÁ PRONTA? LIMA, Ana Paula Moraes de Canto et. ali. São Paulo: Literare Books International, 2020, p. 138.

[20] Portaldaindustria.com.br. Notícias. Pequenas empresas têm tratamento especial na LGPD na Europa e Austrália. Janeiro, 2021. Artigo que traz resultados de pesquisa realizada sobre o tratamento diferenciado às pequenas empresas em 27 países europeus e na Austrália. Disponível em: < https://noticias.portaldaindustria.com.br/noticias/economia/pequenas-empresas-tem-tratamento-especial-na-lgpd-na-europa-e-australia/>. Acessado em 10 fev. de 2021.

[21] Disponível em: <https://datasebrae.com.br/totaldeempresas/>. Dados de maio, 2020. Acessado em 10 fev. de 2021.

Por outro lado, segundo levantamento da Associação Brasileira de Startups - Abstartups[22], existem mais de 12.700 empresas classificadas como startups no país. Segundo o Perfil da Startup Brasileira (Radiografia do Ecossistema Brasileiro de Startups[23]), 63% das startups contam com até 05 pessoas, 49% são compostas apenas pelos sócios, 69% tem faturamento abaixo de R$ 50.000,00 e 15% possuem faturamento entre R$ 50.000,00 e R$ 250.000,00 anuais, 69% tem até 03 anos de funcionamento e apenas 69,7% possuem o CNPJ formalizado junto aos órgãos oficiais.

Ainda segundo a radiografia, 16,2% atual no ramo de serviços profissionais, 11% no ramo de TI e Telecomunicações, 8,8% em serviços financeiros, 8,2% em saúde, 7,5% em varejo ou atacado e 7% em educação. As demais possuem menores participações em atividades como mobilidade, entretenimento, turismo, agronegócios, *lawtechs* etc.

Todavia, um aspecto relevante foi identificado quando se fala em *compliance* com a LGPD, a adoção de melhores práticas de governança de dados e de necessidade de um sistema de gestão da segurança da informação.

Conforme a radiografia, 36,9% das startups operam com *Analytics* e *Big Data*, 23% trabalham com Clouds, 13,7% com Inteligência Artificial. Ainda é importante destacar que em mais de 55% dos casos, as startups possuem consumidores finais em sua cadeia de tratamento de dados, direta ou indiretamente. Esse panorama, em tese, revela que as startups, diferentemente das micro e pequenas empresas, em geral, são mais vocacionadas à tecnologia e tratam dados em maior escala, apontando para que a abordagem regulatória, neste aspecto, seja calibrada em função dos riscos potenciais acarretados ou possíveis pela atividade desenvolvida pelo controlador e ameaças aos direitos ou liberdades individuais[24].

Por isso, na Europa, devem nomear encarregado de dados, atividades cujo exercício se sujeita à regulação, tais como do ramo de finanças, corretoras, seguridade, jogos eletrônicos, atividades sujeitas às leis de prevenção e combate à lavagem de capitais e financiamento ao terrorismo, saúde, ensino, empresas de

---

[22] G1.Globo.com. Globonews. Número de startups no Brasil aumento 20 vezes nos últimos oito anos. 11 já são unicórnios. Disponível em: <https://g1.globo.com/globonews/noticia/2020/01/15/numero-de-startups-no-brasil-aumentou-20-vezes-nos-ultimos-oito-anos-11-ja-sao-unicornios.ghtml>. Acessado em 10 fev. de 2021.

[23] O Momento da Startup Brasileira e o futuro do Ecossistema de Inovação. 2017. Mapeamento disponibilizado pela Abstartups em: <https://abstartups.com.br/radiografia-do-ecossistema/>. Acessado e download em 10 fev. de 2021.

[24] É como o tema vem sendo abordado, sob o ponto de vista regulatório, nas jurisdições europeias, segundo os *guidelines* e legislações de cada um dos países, adequando as realidades locais à GDPR. Por exemplo Espanha e Portugal, jurisdições nas quais as empresas de pequeno porte somente precisam designar um Encarregado de Proteção de Dados quando tratarem "dados sensíveis", dados relacionados a condenações criminais, ou tratarem dados "em larga escala" (arts. 9 e 10, do RGPD). Na maioria dos países da Europa, também, são obrigadas a nomear o Encarregado as empresas cujas atividades principais sejam o "processamento de dados pessoais", ou seja, o principal negócio das mesmas, e, ainda, que tal exposição possa acarretar ameaças a direitos e liberdades individuais. Ver mais em: <https://blog.privacyperfect.com/gdpr-for-smes-key-points>; <https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/>; e https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos>. Acessado em 11 fev. de 2021.

comunicação, meios de comunicação, marketing, investigação de mercado, pesquisas e, também, as que trabalham com algoritmos que formam perfis de consumidores.

Uma exceção que se vislumbra, segundo os *guidelines* das autoridades europeias, seria em relação a empresas com menos de 250 colaboradores. Todavia, há a ressalva legal ou regulamentar quanto ao potencial risco de ameaça a direitos e liberdades individuais e as que trabalham "em larga escala" com dados pessoais.

Na avaliação de Claudinei Vieira, o risco relacionado à proteção da privacidade e da segurança de dados pessoais, não necessariamente é proporcional ao porte da empresa controladora. Por exemplo, menciona o autor, as microempresas, startups e consultorias especialistas, de pequeno porte, que tratam milhões de dados pessoais, diariamente, que vão de dados cadastrais, transacionais e até dados sensíveis[25]

Poder-se-ia trazer para nossa realidade, então, o que se passa com as startups, conforme a radiografia e o perfil acima comentados. Aquelas startups cujo negócio principal seja o tratamento para si própria ou para seus clientes (B2B ou B2C) de dados pessoais, deveriam nomear Encarregado de Dados[26]. Em qualquer hipótese, micro e pequenas empresas, que também exercerem essas atividades (não necessariamente definidas como startups), deveriam nomear um Encarregado de Dados.

Ainda quanto a dados de crianças e adolescentes e dados sensíveis, toda empresa ou agente de tratamento deverá nomear encarregado de dados, ou, se preferir, contratar assessoria especializada no mercado com essa finalidade.

Nossa sugestão, no tocante a assessorias especializadas, é que tais entidades devam passar por algum tipo de certificação e obtenção de registro prévio, com revalidação periódica, junto à ANPD.

Sob a ótica de melhores práticas e governança de dados, a ANPD deveria expedir regulamentação facultando a designação de profissional encarregado de dados com a autonomia técnica e acesso diretamente aos diretores e proprietários, para empresas com porte a partir de médio. No caso de startups, com vocação tecnológica, a regulamentação poderia facultar que as empresas com mais de 50 (cinquenta) colaboradores adotem o mesmo sistema de governança de dados e designação de profissional com autonomia técnica, independente do faturamento da startup.

Nesse sentido, verifica-se, em outras jurisdições, cautelas com empresas que tratam dados pessoais em larga escala[27] ou que ofereçam riscos potenciais. Segundo a Autoridade de Dados da Estônia, por exemplo, o tratamento de dados pessoais em larga escala pode ser assim considerado quando inclui: a) categorias especiais de

---

[25] LGPD: Lei Geral de Proteção de Dados Pessoais. Manual de Implementação. MALDONADO, Viviane Nóbrega (Coord). São Paulo: Thomson Reuters Brasil, 2019, p. 43.

[26] Segundo Claudinei Vieira, idem, este contexto é desafiador para as startups, pois a coleta de dados pessoais, o uso de algoritmos, a existência de equipes de desenvolvimento, o uso de internet das coisas, a necessidade de sistema de gestão de segurança da informação e o uso de plataformas em clouds são pontos de atenção para esse tipo de atividade. p. 45.

[27] Por exemplo, a Estônia, que já em 2018 lançou *guidelines* acerca de delimitar e melhor conceituar o que seria tratamento de dados "em larga escala", conforme disponível em: <https://inplp.com/latest-news/article/the-estonian-data-protection-authority-issued-guidance-on-the-definition-of-large-scale-processing/>. Acessado em 11 fev. de 2021.

dados pessoais (por exemplo dados sensíveis, menores e adolescentes etc.) ou, ainda, dados pessoais relacionados a processos criminais de um universo superior a 5.000 (cinco mil) titulares; b) dados pessoais classificados como de alto potencial de risco de um universo superior a 10.000 (dez mil) titulares; e, finalmente, c) outras categorias de dados pessoais de um universo de tratamento superior a 50.000 (cinquenta mil) titulares[28].

No caso de empresas que exerçam atividades reguladas, sejam quaisquer que sejam essas atividades, ouvida a entidade reguladora setorial ou de classe, a ANPD poderá dispensar a nomeação de Encarregado de Dados ou contratação de assessoria especializada, sempre que o porte dos agentes sob questão for Micro ou Pequena Empresa, ou, de qualquer porte, com atendimento das seguintes situações alternativas: a) contem com menos de 20 (vinte) colaboradores, ou b) tratem mensalmente dados pessoais de menos de 5.000 (cinco mil) titulares. Enquadrar-se-iam no exercício de atividades profissionais reguladas todas as atividades sujeitas à inscrição em Conselhos Profissionais de Classe e, também, a advocacia, sejam mediante sociedade, sociedade unipessoal ou pessoa física.

Não se aplicaria nenhuma dispensa quando os dados se relacionarem a crianças e adolescentes ou os dados forem classificados como dados sensíveis.

Quanto aos agentes de pequeno porte, MEI e Micros e Pequenas Empresas que exerçam atividades não sujeitas a regulação, e não se definam como startups, a ANPD poderia expedir regulamentação dispensando a nomeação de Encarregado de Dados de todas as pessoas físicas, as MEI e as EIRELI. No caso de demais espécies de Pessoas Jurídicas e Sociedades, ou seja, as cujo faturamento as classifique como Pequenas e Médias, a dispensa poderia ser mediante o atendimento, alternativo, de uma das seguintes condições: a) contém com até 100 (cem) colaboradores; ou b) tratam dados pessoais, mensalmente, de até 5.000 (cinco mil) titulares. Igualmente, não se aplicaria nenhuma dispensa quando os dados se relacionarem a crianças e adolescentes ou os dados forem classificados como dados sensíveis.

Opta-se, nestas proposições, por parâmetros mais rígidos e menos elastecidos que os empregados na Europa e, também, quanto aos adotados na Estônia, tendo em consideração dois fatores: a) a cultura de proteção de dados pessoais e a evolução digital naqueles mercados são drasticamente superiores, no atual estado da arte, à realidade brasileira, principalmente longe dos grandes centros urbanos; b) os marcos regulatórios já vigem por lá há pelo menos 5 anos, e mais fortemente, nos últimos 3 anos, com regulamentações expedidas e ações já empreendidas pelas autoridades de fiscalização e supervisão.

Presume-se, então, que entre nós caberia dar um tratamento baseado nos riscos (*Based Risk Approach*), no caso de atividades que se utilizem de sítios eletrônicos ou APP que coletem dados pessoais, mediante preenchimento de formulários ou mediante cookies. Podem aí se enquadrar o *e-commerce* em geral, por exemplo, ainda que mediante contratação de empresas fornecedoras de tecnologia ou de plataformas de serviços (*SaaS ou PaaS*).

É que, segundo a definição do artigo 46, da LGPD, os agentes de tratamento, ou seja, aqueles que tratam os dados nas suas atividades principais por si ou por delegação, devem adotar as medidas de segurança, técnicas e administrativas aptas

[28] INPLP.com, Idem.

à proteção dos dados por eles tratados e custodiados[29]. Logo, dados de *prospects* ou de clientes e consumidores, são dados pessoais resguardados pela regulamentação, cujos titulares desfrutam do pleno exercício de seus direitos, e a designação de um Encarregado de Dados, seria uma providência recomendável para facilitação desses direitos[30], inclusive no tratamento de incidentes e comunicações consequentes (art. 48[31]).

De lege ferenda, pois, vislumbra-se a necessidade de inclusão de textos nos seguintes artigos da LGPD:

> **Artigo 41 – O controlador, em qualquer caso, e o operador, este último segundo diretrizes da autoridade nacional, deverão indicar encarregado pelo tratamento de dados pessoais.**
>
> **§ 1º A identidade (pessoa física ou jurídica) e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do agente de tratamento.**
>
> **(...)**
>
> **(Novo) § 4º Não serão objeto de dispensa do dever de designação de encarregado, pela autoridade nacional, nas hipóteses do parágrafo anterior, quando o tratamento de dados pessoais se relacionarem a: I – dados sensíveis; II – dados de crianças e adolescentes, e III – dados relacionados a processos criminais.**
>
> **(Novo) § 5º Para a expedição de normas regulamentares sobre dispensas da designação de encarregado, bem como sobre outras atribuições, sempre que a atividade objeto da norma for regulada por entidade de classe ou por órgão regulador da esfera federal, a autoridade nacional deverá, previamente, ouvir as respectivas instituições.**

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

De acordo com o art. 37 da Lei 13.709/2018, o controlador e o operador de dados pessoais devem manter o registro das operações de tratamento. Esse registro envolve a criação e manutenção regular de relatórios capazes de descrever, entre outros aspectos: (i) quais são os dados coletados; (ii) a forma da captura; (iii) o local de seu trânsito ou armazenamento dentro da organização; (iv) as finalidades do tratamento; (v) as medidas de segurança da informação em cada operação; e (vi) as bases legais que justificam o tratamento de dados.

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

[30] Vide também os artigos 5º, V, 18 e 47, todos da LGPD.

[31] Artigo 48, LGPD: O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Para que esses registros sejam fidedignos, é essencial que exista um processo organizado para que um levantamento inicial seja realizado, sendo esse processo normalmente chamado de mapeamento de dados pessoais (ou "*data mapping"*). O grande desafio é o nível de detalhamento necessário para que esse processo seja feito da melhor forma possível, normalmente demandando um complexo processo de levantamento de dados e informações, além do estabelecimento de critérios para utilização dos dados e bases legais de tratamento adequadas para cada operação.

Além disso, esse processo deve se dar de forma contínua, não bastando que o processo seja realizado uma única vez, mas demandando atualização a cada nova operação ou modificação de operações existentes.

O processo descrito acima é um dos principais gargalos em projetos de adequação em proteção de dados para qualquer organização, demandando um esforço considerável das suas estruturas organizacionais para que os dados sejam levantados e registrados. Independentemente do porte da empresa ou seu faturamento, fato é que quanto maior a complexidade dos processos organizacionais da empresa em relação ao fluxo de dados pessoais empregados nas atividades, mais complexo e se prolongado no tempo será esse levantamento.

Para agentes de pequeno porte, o impacto do registro das operações de tratamento pode assumir duas características, a depender do grau de complexidade das operações do agente:

a) Agentes de pequeno porte com operações de **baixa complexidade,** aqui consideradas aqueles que não utilizam: (i) ferramentas automatizadas de tratamento; (ii) múltiplos bancos de dados; (iii) em regra, dados pessoais sensíveis; (iv) atividades com finalidade de geração de leads/marketing digital para si próprio ou para terceiros. Nesses casos, o registro das operações gera um impacto relativamente pequeno na organização, pois trata-se de levantamento de operações normalmente pouco complexas e com bases legais de fácil percepção. Ainda assim, devemos considerar que esses agentes contam com pouca ou nenhuma disponibilidade de recursos para promover esse processo de adequação, além de que seus esforços normalmente estão muito concentrados em atingir os propósitos fundamentais da organização – como investimento em vendas, marketing, matérias-primas e mão-de-obra. Por fim, a princípio, a ausência de registros precisos a respeito das operações de tratamento possui baixo potencial de causar danos ao titular dos dados pessoais.

b) Agentes de pequeno porte com operações de **alta complexidade,** aqui consideradas aqueles que utilizam: (i) ferramentas automatizadas de tratamento; (ii) múltiplos bancos de dados; (iii) em regra, dados pessoais sensíveis; (iv) com finalidade de geração de leads/marketing digital para si próprio ou para terceiros. Assim como nas organizações com operações de baixa complexidade, esses agentes normalmente contam com pouca ou nenhuma disponibilidade de recursos para promover esse processo de adequação, porém há de ser considerado que as operações são normalmente mais complexas e podem gerar mais riscos ao titular de dados, e consequentemente mais riscos para o próprio agente de tratamento. Por essa razão, parece razoável supor que deve haver um

interesse no registro dessas operações para mitigação de riscos, sendo o principal impacto para o agente o investimento necessário para a realização dessas atividades.

Nesse sentido, no contexto dos obstáculos às atividades de MPs e EPPs, pode-se considerar como principais impactos causados pela exigência prevista no art. 37, da LGPD: (i) complexidade do tema; (ii) necessidade de apoio técnico especializado; (iii) aumento de custos fixos do agente de pequeno porte; (iv) desconexão das finalidades do tratamento de dados pessoais com a atividade principal do negócio.

Assim, entende-se relevante apresentar essas ponderações à ANPD, para que sejam consideradas na formação de normas capazes de estabelecer critérios para o abrandamento de obrigações legais atinentes à formalização de registro nas operações de tratamento de dados pessoais executadas por MPs e EPPs.

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

O relatório de impacto à proteção de dados está previsto no art. 38 da Lei Geral de Proteção de Dados como um documento que destinado a demonstrar os dados coletados, a metodologia utilizada no tratamento dos dados pessoais e as medidas de segurança e salvaguardas para mitigação de riscos da operação.

O relatório de impacto à proteção de dados impacta os agentes de pequeno porte na medida em que pressupõe dessas organizações alto grau de conformidade com a Lei Geral de Proteção de dados, principalmente por pressupor a existência de uma análise prévia em relação a viabilidade da operação de tratamento.

Para que o agente possa entregar o relatório, é essencial que tenha todas as suas operações mapeadas e registradas, com as devidas bases legais de tratamento de dados definidas, além das medidas de segurança adotadas. Só assim será possível, em um primeiro momento, determinar quais operações de risco demandam um relatório de impacto detalhado e, na sequência, o desenvolvimento do referido relatório.

Como principal impacto para os agentes de pequeno porte está a necessidade de um profissional especializado que possa avaliar as operações de tratamento que demandem a geração do relatório, bem como a realização de testes de ponderação entre as finalidades e necessidades do tratamento em contraposição aos direitos e garantias fundamentais do titular de dados.

Tal atividade é complexa e demanda apoio técnico especializado, que nem sempre será considerado viável ao agente de pequeno porte.

Nesse sentido, são os principais impactos:

a) Necessidade de maturidade da organização em termos de proteção de dados;

b) Dependência da observância de outros pontos da legislação para que seja possível gerar o relatório;

c) Necessidade de apoio técnico especializado (interno ou externo);

d) Planejamento estratégico bem definido

Assim, entende-se relevante apresentar essas ponderações à ANPD, para que sejam consideradas na formação de normas capazes de estabelecer critérios para o abrandamento de obrigações legais atinentes à formalização de registro nas operações de tratamento de dados pessoais executadas por MPs e EPPs.

Quais os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?

A Lei Geral de Proteção de Dados (LGPD) confere ampla proteção ao direito à privacidade e proteção de dados pessoais, recaindo sobre todos aqueles que realizem atividade de tratamento de dados pessoais, abrangendo os mais diversos setores da economia, tanto no âmbito público quanto no âmbito privado.

Do texto da Lei 13.709/2018, conclui-se sua aplicação a todas as pessoas físicas ou jurídicas que realizem quaisquer das atividades de tratamento de dados pessoais elencadas em seu artigo 1º, impactando de igual modo empresas de grande e pequeno porte, independentemente de usa natureza jurídica ou segmento de atuação.

O tratamento diferenciado para as micro e pequenas empresas previsto na constituição, também contemplando na LGPD é uma realidade em outros países com legislações mais avançadas. Na Europa, empresas com menos de 250 empregados não precisam manter registro das operações de tratamento de dados pessoais que realizem a menos que o processamento de informações seja a atividade regular da empresa, com real potencial de dano ao consumidor. Também, as empresas de pequeno porte estão eximidas de nomear um profissional específico para gerenciar o tratamento de dados.

Na lei brasileira, em que pese a previsão do inciso XVIII, do artigo 55-J, que incumbe a Agência Nacional de Proteção de Dados editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para os agentes de pequeno porte possam se adequar às disposições da lei, não há, ainda, exceção neste sentido.

A postergação da aplicação das sanções previstas na Lei Geral de Proteção de Dados Pessoais para agosto de 2021, não elide as microempresas e pequenas de pequeno porte à observância das disposições da lei diante dos demais riscos a que estão sujeitadas desde a sua vigência, sendo possível sua exigibilidade em outros âmbitos.

Os riscos inerentes a não adequação à Lei Geral de Proteção de Dados demandam a estruturação de programa de governança de dados que estabeleça boas práticas, normas de segurança e mitigação de riscos no uso e no tratamento de dados pessoais.

O gerenciamento de dados pessoais é, portanto, fator importante a ser considerado diante dos riscos implicados. No caso de violação às normas previstas na lei, as penalidades variam desde uma simples advertência até a eliminação dos dados que foram objeto da infração. As multas pecuniárias previstas na lei podem recair sobre 2% do faturamento anual da companhia limitada a 50 milhões de reais por infração. Conforme disposto no parágrafo primeiro do artigo 52 da lei, as sanções serão aplicadas de forma gradativa em conformidade com o caso concreto, devendo ser considerados alguns parâmetros e critérios dentre os quais se incluem a adoção de mecanismos e procedimentos internos orientados à mitigação do dano, voltados ao tratamento seguro e adequado de dados e a adoção de boas práticas de governança.

A adoção de adequada política de dados, que contemple a criação de fluxos e procedimentos internos que permitam controlar as atividades de tratamento de dados pessoais durante todo o seu ciclo de vida no âmbito interno da empresa é de fundamental importância repercutindo na gradação da sanção aplicável em decorrência de violação de dispositivo da lei.

Apesar de a lei apontar o caminho a ser trilhado para a conformidade e aplicação das disposições legais relacionadas às boas práticas, a cultura de governança de dados é ainda incipiente no Brasil. Parcela significativa das empresas de pequeno e médio porte considera irrelevante ou desnecessária a aplicação de medidas de segurança da informação, conformidade e prevenção de riscos, frequentemente relacionando a estruturação de um programa de governança de dados a gastos financeiros desproporcionados ou a processos complexos que inviabilizem a operacionalidade do negócio.

As micro empresas ou empresas de pequeno porte tem o desafio de organizar um plano de adequação à Lei Geral de Proteção de Dados alinhando à governança de dados e boas práticas de gestão, muitas das vezes pouco desenvolvidas ou estruturadas no âmbito das microempresas e empresas de pequeno porte, de modo adequado ao modelo de negócios desenvolvido e à realidade financeira da empresa.

De outra parte enfrentam a escassez de profissionais e de expertise para orientá-las quanto à conformidade à LGPD o que impacta implementação de programas de governança de dados, em razão das eventuais dificuldades na descrição dos processos das atividades de tratamento de dados e na identificação das bases legais que as autorizem. A mudança de cultura imposta pela LGPD acarreta custos financeiros que incidem desproporcionalmente sobre empresas de menor porte.

A qualidade de microempresa ou empresa de pequeno porte[32] não pressupõe, necessariamente, tratamento reduzido de dados pessoais, pode ocorrer que agente de pequeno porte realize grande volume de atividade de tratamento de dados pessoais e, ainda assim, tenham orçamento e estrutura reduzidos. O risco pode ser, portanto, desproporcional

Se por um lado os agentes de pequeno porte podem sofrer impacto financeiro importante em decorrência da implementação de programa de governança de dados, podendo afetar a viabilidade de sua atividade; por outro, a implementação de programa de governança de dados pode beneficiar os pequenos negócios, na medida

[32] Conforme o conceito do artigo 3º da Lei Complementar 123/2006.

em que boas práticas de governança permitem a redução de hipóteses vazamentos ou outros incidentes envolvendo dados pessoais, mitigando o risco assumido pela empresa no desenvolvimento de sua atividade, incluindo-se o risco reputacional derivado.

O equilíbrio entre as soluções a serem adotadas pelas microempresas e empresas de pequeno porte quanto a governança de dados passa, invariavelmente, pela atividade da ANPD. Estabelecer parâmetros e critérios para definição de agente de pequeno porte para os efeitos da Lei Geral de Proteção de Dados seja, talvez, o primeiro desafio a ser superado, justamente em razão da desproporcionalidade do risco na gestão de dados.

Nesse sentido, a atuação da ANPD Dados será fundamental para aplicação da lei, bem como para o desenvolvimento de orientações e ações afirmativas voltadas ao desenvolvimento da cultura da proteção de dados e a edição de procedimentos simplificados dirigidos aos agentes de pequeno porte.

A Comissão Europeia disponibiliza em seu endereço eletrônico orientação em linguagem simplificada dirigida às pequenas empresas sobre o Regulamento Europeu de Proteção de Dados, explicando conceitos, incentivando a mudança de paradigma quanto ao tratamento de dados pessoais, apontando diretrizes a serem adotadas pelas empresas e recomendando a adoção de procedimentos simplificados[33].

Em conclusão, há que se levar em consideração que os impactos da implementação do programa de governança de dados aos agentes de pequeno porte passam, antes de mais nada, pela identificação e registro dos atos de tratamento de dados pessoais, conforme abordado anteriormente, de modo que as contribuições apresentadas naquele tópico podem ser reaproveitadas na análise deste quesito.

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

A LGPD está movimentando todos os setores, seja público ou privado, e portes de empresas, desde às microempresas até empresas de grande porte. Observa-se que de um modo geral, o foco tem sido os aspectos jurídicos da LGPD, mas o que muitos esquecem ou ainda não perceberam é que a LGPD é uma lei de implementação tecnológica.

Há que se lembrar também que a LGPD carrega em seu bojo aspectos não somente jurídicos, mas um arsenal de termos técnicos da área de Segurança da Informação associados aos termos básicos da área de Ciência da Computação como um todo. Os termos: coleta de dados, tratamento de dados, anonimização, bloqueio, prevenção, riscos, medidas, salvaguardas e mecanismos de mitigação de riscos e relatórios de impacto à proteção de dados pessoais. Esses são alguns exemplos de aspectos tecnológicos que permeiam o texto legislativo.

[33] Disponível em: https://ec.europa.eu/justice/smedataprotect/index_pt.htm.

Todos esses elementos são importantes frente ao interesse de proteger dados e garantir a privacidade como direito fundamental para todos os titulares de dados.[34]

Inicialmente deve-se ter em mente que os dados possuem um ciclo de vida, ou seja, desde seu nascimento (coleta) até sua morte (eliminação). A LGPD estabelece uma relação entre o ciclo de vida dos dados por meio da definição de "tratamento de dados" (LGPD, art. 5º, inciso X).

As operações indicadas na LGPD não compreendem o conjunto completo de operações passíveis de realização a partir de dados pessoais ou sensíveis, sendo o rol meramente exemplificativo. Mas é importante notar que o texto legislativo não se prende às técnicas ou aos métodos computacionais ou operacionais, uma vez que a partir de determinadas operações exemplificadas no art. 5º, inciso X, pode-se realizar desde a captura do dado até a aplicação de técnicas de Mineração de Dados (*Data Mining*) ou Aprendizagem de Máquina (*Machine Learning*).

Portanto, ciclo de vida e tratamento de dados estão relacionados à aspectos de Segurança da Informação, visto que não se pode proteger dados pessoais esquecendo-se da segurança. Assim a Norma ABNT NBR ISO/IEC 17799[35] define Segurança da Informação como:

> "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."

E, neste sentido, a Segurança da Informação tem por base algumas propriedades, a saber: "preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas"[36].

Tais propriedades constam definidas na Norma ISO/IEC 13335-1[37]:

---

[34] FREITAS, Cinthia Obladen de Almendra. O que está em jogo no vazamento de milhões de CPFs? ESTADÃO, 26 jan. 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/o-que-esta-em-jogo-no-vazamento-de-milhoes-de-cpfs/. Acesso em: 15 fev. 2021.

[35] A partir de 2007, a norma ISO/IEC 17799 foi incorporada ao novo sistema de numeração de normas, passando a constar como ISO/IEC 27002. ABNT NBR ISO/IEC 17799. Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. 2005. p. ix.

[36] A partir de 2007, a norma ISO/IEC 17799 foi incorporada ao novo sistema de numeração de normas, passando a constar como ISO/IEC 27002. ABNT NBR ISO/IEC 17799. Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. 2005. p. 01. Disponível em: <http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acesso em: 15 jan. 2021.

[37] ISO/IEC 1333-1. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and

a) disponibilidade[38]: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
b) confidencialidade[39]: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
c) integridade[40]: propriedade de salvaguarda da exatidão e completeza de ativos;
d) autenticidade[41]: propriedade de salvaguarda da veracidade ou originalidade de ativos. Propriedade que garante que a identidade de um sujeito ou recurso seja a reivindicada. Autenticidade se aplica a entidades como usuários, processos, sistemas e informações;
e) não repúdio[42]: a capacidade de provar que uma ação ou evento ocorreu, para que esse evento ou ação não possa ser repudiado antes, ou seja, não se pode negar a existência de um fato;
f) confiabilidade[43]: propriedade que se refere aos comportamentos e resultados pretendidos consistentes.

E, a Segurança da Informação está a cada dia mais em evidência com a entrada em vigor da LGPD. E, entre a proteção de dados e a segurança da informação, há que se entender que a proteção é sobre os dados (unidade originária, o dado), mas a segurança considera uma abrangência maior, ou seja, os dados, os sistemas, os processos e a organização como um todo. Por isso, o art. 6º, incisos VII e VIII, da LGPD apontam que:

> "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;"

Por isso, as normas ISO/IEC da família 27000 foram preparadas para "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)."[44]

---

communications technology security management. 2004. p. 03. Disponível em: <https://www.iso.org/standard/39066.html>. Acesso em: 15 jan. 2021.

[38] Texto original: the property of being accessible and usable upon demand by an authorized entity.

[39] Texto original: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

[40] Texto original: the property of safeguarding the accuracy and completeness of assets.

[41] Texto original: the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information.

[42] Texto original: *the ability to prove an action or event has taken place, so that this event or action cannot be repudiated before. Ver também: ISO/IEC 13888-1. Information technology — Security techniques — Non-repudiation — Part 1: General. 2009.*

[43] Texto original: the property of consistent intended behaviour and results.

[44] Texto original: This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). ISO/IEC 27001. Information technology — Security techniques —

Assim, as normas relacionadas à Segurança da Informação não mencionam dados ou informações, mas ativos que representam "qualquer coisa que tenha valor para a organização"[45].

Deste modo, do ponto de vista tecnológico, a LGPD aponta como aspecto formal a manutenção de registro das operações de tratamento de dados por parte tanto do controlador quanto do operador, ou seja, pelos agentes de tratamento de dados, especialmente quando o tratamento tiver por base o legítimo interesse (artigo 37, LGPD).

Neste encadeamento de soluções tecnológicas, a LGPD não deixou de considerar os princípios da responsabilização e da prestação de contas, pelos quais preconiza a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (art. 6º, inciso X). Há, portanto, um ciclo tecnológico que se estabelece a partir da LGPD visando a proteção de dados com base na Segurança da Informação.

Alguns dados apresentam-se relevantes nesta discussão voltada aos agentes de tratamento de dados em empresas de pequeno porte. O Comitê de Pequenas Empresas do Congresso dos Estados Unidos descobriu que 71% dos ataques cibernéticos aconteceram em empresas com menos de 100 funcionários.[46] Tal documento mostra que erroneamente os empresários de empresas de pequeno porte pensam que ciberataques não ocorrem e cibercriminosos não se interessam por este tipo de empresa e seus dados.

Contrariamente, as empresas de pequeno porte se preocupam menos e aplicam em menor escala medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A atuação é reativa e não preventiva, de modo que sejam adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

O Comitê de Pequenas Empresas do Congresso dos Estados Unidos mostra que as empresas de pequeno porte utilizam redes menos seguras, tornando mais fácil violar a rede e, consequentemente, vazar dados pessoais.[47]

Muitos são os fatores que influenciam a não Segurança da Informação nas empresas de pequeno porte, a exemplo de: falta de tempo, orçamento pequeno e a não experiência voltada à Segurança da Informação, ausência de um especialista em segurança de Tecnologia da Informação (TI), não estar ciente dos riscos, falta de treinamento dos funcionários, não atualizar os *software* de segurança, terceirizar a

---

Information security management systems — Requirements. 2013. p. v. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 15 jan. 2021.

[45] ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2013. p. 02. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 15 jan. 2021.

[46] COMMITTEE ON SMALL BUSINESS. Small business, big threat: protecting small businesses from cyber attacks. 2015. Disponível em: https://www.congress.gov/event/114th-congress/house-event/LC30421/text?s=1&r=10. Acesso em: 15 fev. 2021.

[47] Idem.

Segurança da Informação e não proteger adequadamente a rede e o parque tecnológico (incluindo os dispositivos móveis).[48]

Portanto, algumas recomendações podem ser extraídas das normas ISO/IEC da família 27000 visando prover um suporte tecnológico básico aos agentes de tratamento de dados pessoais em empresas de pequeno porte.

A norma ISO 27001 é a norma técnica que trata dos requisitos do Sistema de Gestão de Segurança da Informação (SGCI), projetado pelas empresas para *"assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas"*[49]. A certificação aplicação da norma ISO 27001 é para empresas e a certificação não corresponde à pessoal técnico. Mesmo sendo a certificação uma decisão estratégica e gerencial, cabe destacar que a mesma estabelece o modelo *"Plan-Do-Check-Act"* para estruturar os processos do SGSI. O modelo PDCA estabelece um ciclo contínuo de "planejar-implementar e operar- monitorar e analisar criticamente- manter e aprimorar" o SGSI.

A Tabela 01 relaciona a LGPD, por meio de 03 (três) aspectos relevantes: (i) boas práticas de governança, (ii) manutenção de registro de operações e (iii) segurança e sigilo de dados; e os itens relevantes do Anexo A da norma ISO/IEC 27001.

Tabela 01: Relação entre LGPD e ISO/IEC 27001

LGPD	ISO/IEC 27001 (Anexo A)
Boas práticas de governança - CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS - Seção II Das Boas Práticas e da Governança (artigos 50 e 51)	A.5 – Políticas de segurança da informação A.14 – Aquisição, manutenção e desenvolvimento de sistemas A.17 – Aspectos da segurança da informação na gestão da continuidade do negócio A.18 - Coformidade
Manutenção de registros de operações - CAPÍTULO VI DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS - Seção I Do Controlador e do Operador (artigos 37 ao 40)	A.8 – Gestão de ativos A.13 – Segurança nas comunicações
Segurança e sigilo de dados - CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS - Seção I Da Segurança e do Sigilo de Dados (artigos 46 ao 49)	A.9 – Controle de acesso A.10 – Criptografia A.12 – Segurança nas operações A.14 – Aquisição, manutenção e desenvolvimento de sistemas

[48] ARMERDING, Taylor. Why criminals pick on small business. 2015. Disponível em: https://www.csoonline.com/article/2866911/why-criminals-pick-on-small-business.html. Acesso em: 15 fev. 2021.

[49] ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2013. p. 01. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 15 jan. 2021.

A vantagem da utilização da norma ISO 27001, como um modelo de pensar a Segurança da Informação, é que a mesma protege e aplica-se a todo e qualquer conteúdo e formato de dados, esteja este armazenado ou não em meios físicos ou digitais, garantindo a sua proteção independentemente do seu formato ou meio de armazenamento utilizado. Tal qual preconizado na LGPD.

Um olhar especial cabe também à norma ISO 27701[50], a qual objetiva aprimorar o SGSI já existente nas organizações, com requisitos adicionais e que tratam especificamente da privacidade de dados. Isto no intuito de estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Informações de Privacidade – SGIP.

O referido padrão estabelece uma estrutura para que os agentes de tratamento de dados (art. 5º., inciso VI a VIII) possam estabelecer mecanismos de controles de privacidade e redução de riscos de violação aos direitos da privacidade.

Assim, considerando que a LGPD objetiva *"*proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*"* (art. 1º) e fundamenta-se na proteção da privacidade, da inviolabilidade da intimidade, da honra e da imagem, dentre todos os demais fundamentos dos incisos do art. 2º, entende-se que a norma ISO 27701 vem em momento oportuno apoiar o ferramental tecnológico e normativo.

A Tabela 02 relaciona a LGPD, por meio de 04 (quatro) aspectos relevantes às empresas de pequeno porte: (i) coleta e tratamento de dados, (ii) titulares de dados pessoais, (iii) *privacy by design/by default* e (iv) compartilhamento, transferência e divulgação de dados pessoais; e os itens relevantes da norma ISO/IEC 27701 no que tange aos agentes de tratamento de dados.

Tabela 02: Relação entre LGPD e ISO/IEC 27701

LGPD	ISO/IEC 27701
Coleta e tratamento de dados	Condições para coleta e tratamento: 7.2 – Controlador e 8.2 – Operador
Titulares de dados pessoais	Obrigações para os titulares de dados pessoais: 7.3 – Controlador Obrigações dos titulares de dados pessoais: 8.3 – Operador
Privacy by design/by default	Condições para coleta e tratamento: 7.4 – Controlador e 8.4 – Operador
Compartilhamento, transferência e divulgação de dados pessoais	Compartilhamento, transferência e divulgação: 7.5 – Controlador e 8.5 – Operador

Destaca-se que mesmo havendo um SGSI abrangente e alinhado à ISO/IEC 27001, deve-se esclarecer que os requisitos de tal norma podem ser atendidos sem que a privacidade como um todo esteja devidamente protegida e que mecanismos voltados especificamente à esta questão tenham sido implementados. A LGPD menciona "medidas, salvaguardas e mecanismos de mitigação de risco", art. 5º -

[50] ISO/IEC 27701. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. 2019. Disponível em: <https://www.iso.org/standard/71670.html>. Acesso em: 15 jan. 2021.

inciso XVII e princípios da segurança e da prevenção, art. 6º - incisos VII e VIII, mas tal proteção vai muito além de simplesmente proteger os dados propriamente ditos, visto que as empresas de pequeno porte também precisam garantir os direitos dos titulares de dados, o que não pode ser implementado somente por meio da segurança da informação.

Por outro lado, a norma ISO 27701 não só ajudará a organizar as responsabilidades como também servirá de apoio fundamental para responder os pedidos de esclarecimentos por parte da Autoridade Nacional de Proteção de Dados. Isto devido ao fato de que a norma ISO 27701 define os requisitos extras para um SGSI, a fim de proteger a privacidade e tratamento do que é denominado na norma de *Personally identifiable information* (PII)[51], ou seja, Informações de identificação pessoal. Este termo foi tomado pela norma ISO 27701 a partir da definição existente na norma ISO 29100 e é apresentado na GDPR como dado pessoal.

Finalmente, um aspecto da Tabela 02 necessita de atenção, qual seja o item referente à *privacy by design / by defalut.* Os itens 7.4 e 8.4, da norma ISO/IEC 27701, apresentam como objetivo:

> assegurar que os processos e os sistemas sejam projetados de forma que a coleta e o tratamento de DP52 (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.

A norma menciona “sistemas sejam projetados” remetendo às das etapas de desenvolvimento de *software*, seguindo o guia SWEBOK[53], a saber: *software design* (fase de projeto), *software requirements* (requisitos e necessidades), *software process* (durante o desenvolvimento) e *software construction* (fases de validação, testes de unidades, integração e depuração).: *software design*, *software requirements*, *software process* e *software construction*. E a conexão entre a LGPD e o desenvolvimento de sistema estabelece-se a partir do artigo 42:

> Artigo 42: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Isso significa que as medidas de proteção aos dados devem ser incorporadas às soluções tecnológicas desde a etapa inicial de projeto de *software* e, portanto,

---

[51] PII - ‘personal data’ in the GDPR. ISO 29100 defines this as “information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal”. Disponível em: <https://www.sis.se/api/document/preview/914169/>. Acesso em: 15 jan. 2021.

[52] DP – A norma ISO/IEC 27701 utilizada a abreviatura DP para dados pessoais

[53] SWEBOK, do inglês *Software Engineering Body of Knowledge*, é um guia para o corpo de conhecimento em Engenharia de Software, patrocinado pelo IEEE (*Institute of Electrical and Electronics Engineering*).

precisam considerar os princípios da *privacy by design / by default*. O conceito *privacy by design* foi cunhado na década de 1990 para definir a incorporação da privacidade à própria tecnologia[54] e pode ser definido como "*an engineering and strategic management approach that commits to selectively and sustainably minimizing information system's privacy risks through technical and governance controls*".[55]

A *privacy by design*[56] tem por base 07 (sete) princípios que podem ser aplicados como uma estrutura geral para integrar a privacidade e a proteção de dados durante os estágios iniciais do *design* de tecnologias da informação e comunicação (TICs), processos organizacionais, arquiteturas em rede e ao aprimorar os sistemas de governança.[57] A discussão de cada um dos princípios da *privacy by design* está além deste estudo, mas pode-se apontar que as empresas de pequeno porte e, principalmente, as startups, apresentarão vantagens competitivas ao incorporarem a privacidade desde o início de suas atividades, bem como vislumbrarem a privacidade como um salto qualitativo independentemente da área de atuação. Para os agentes de tratamento, marca-se o sexto princípio[58] da *privacy by design*, ou seja, o respeito ao usuário (*Respect for the User – Keep it User-Centric*), mantendo os interesses dos titulares de dados como ponto central.

E, ainda, precisarão considerar a privacidade como padrão (*Privacy as the default setting* ou *privacy by default*), a qual representa que nenhuma ação é necessária por parte do usuário do sistema para proteger sua privacidade, a privacidade já está embutida no sistema desenvolvido. E, para tanto, os agentes de tratamento de dados pessoais em empresas de pequeno porte devem adotar algumas práticas:[59] (i) legitimidade e especificação de finalidade, (ii) limitação da coleta de dados pessoais; (iii) minimização de dados; (iv) limitação de uso, retenção e divulgação de dados pessoais, respeitando-se as finalidades relevantes, necessitando de consentimento com exceções a partir da LGPD (art. 4º); (v) participação e acessos individuais dos titulares a seus dados pessoais, permitindo alterações e remoções.

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

A Lei Geral de Proteção de Dados Pessoais – Lei n.º 13.709/2018, estabeleceu as normas gerais para a proteção dos direitos fundamentais de liberdade

[54] MORALES-TRUJILLO, Miguel Ehécatl; GARCÍA-MIRELES, Gabriel Alberto; MATLA-CRUZ, Erick Orlando; PIATTINI, Mario. **A systematic mapping study of privacy by design in software engineering, CLEI Electronic Journal**, v. 22, n. 1, paper 4, April 2019. p.1-29. p. 2.

[55] Tradução livre: uma abordagem de gerenciamento estratégico e de engenharia que se compromete a minimizar seletivamente e de forma sustentável os riscos à privacidade do sistema de informação por meio de controles técnicos e de governança. CAVOUKIAN, Ann. Operationalizing privacy by design: A guide to implementing strong privacy practices. Information and Privacy Commissioner, Ontario, Canada. 2012. p. 8.

[56] CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles - implementation and mapping of fair information practices. 2009. p.1-5.

[57] MORALES-TRUJILLO et al., op. cit., p. 3-4.

[58] CAVOUKIAN, op. cit., p. 12-54.

[59] MORALES-TRUJILLO et al., op. cit., p. 4-6.

e de privacidade dos titulares de dados pessoais. Todavia, em cumprimento aos supramencionados ditames constitucionais e, também, por força das normas relacionadas à Liberdade Econômica, se faz necessário, conforme estabelecido no seu artigo 55-J, XVIII[60] adequar a sua conformidade às empresas de pequeno porte.

Desse modo, na LGPD, dentre os direitos dos titulares de dados, está previsto no artigo 18, inciso V, o direito de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, a **portabilidade dos dados** a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial. A única ressalva imposta à portabilidade são os dados que já tenham sido anonimizados pelo controlador, conforme o artigo 18, §7º, da Lei.

Outrossim, em caso de impossibilidade de adoção imediata de providência da portabilidade por parte do controlador, ele enviará ao titular do dado resposta, onde poderá: (i) comunicar que não é o agente de tratamento de dados; ou (ii) indicar as razões de fato ou de direito que "impedem a adoção imediata da providência" (artigo 18, §4º). A partir da última expressão, é possível interpretar que a portabilidade de dados tratados pelo agente é obrigatória, podendo o processo, no máximo, a partir de razões de fato ou de direito, ser diferido no tempo. De todo modo, o titular tem o direito de peticionar em relação aos seus dados perante a ANPD e organismos de defesa do consumidor (artigo 18, §§1º e 8º)[61].

Ainda no âmbito da LGPD, consoante previsto no artigo 40, poderá, a autoridade nacional 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.

Feitas essas considerações iniciais, surge a questão sobre quais impactos a implantação da portabilidade de dados pessoais poderá causar aos agentes de pequeno porte?

Essa questão se torna relevante, especialmente quando observamos que os pequenos empreendimentos, segundo a Secretaria Especial de Produtividade, Emprego e Competitividade do Ministério da Economia (Sepec/ME), representam 99% dos negócios brasileiros, têm participação de 30% no PIB e são responsáveis por 55% dos empregos gerados no país[62].

---

[60] Art. 55-J. Compete à ANPD:
(...)
XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

[61] PONCE, Paula Pedigoni. Direito à portabilidade de dados: entre a proteção de dados e a concorrência. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/download/521/26/2041. Acessado em: 12 fev. 2021.

[62] MINISTÉRIO DA ECONOMIA. Governo destaca papel da Micro e Pequena Empresa para a economia do país. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/outubro/governo-destaca-papel-da-micro-e-pequena-empresa-para-a-economia-do-pais. Acessado em 14 de fev. 2021

Ademais, conforme já comentado em outro tópico, porém relevante frisar novamente, existem aproximadamente 19.228.000 empresas, sendo que destas, 9.810.400 são MEI (51,02%), 6.586.490 são ME – Microempresas (34,25%)[63].

Por outro lado, como também já registrado, segundo levantamento da Associação Brasileira de Startups - Abstartups[64], existem mais de 12.700 empresas classificadas como startups no país. Segundo a Radiografia do Ecossistema Brasileiro de Startups[65], 63% das startups contam com até 05 pessoas, 49% são compostas apenas pelos sócios, 69% tem faturamento abaixo de R$ 50.000,00 e 15% possuem faturamento entre R$ 50.000,00 e R$ 250.000,00 anuais, 69% tem até 03 anos de funcionamento e apenas 69,7% possuem o CNPJ formalizado junto aos órgãos oficiais.

Ainda segundo a referida radiografia, 16,2% atual no ramo de serviços profissionais, 11% no ramo de TI e Telecomunicações, 8,8% em serviços financeiros, 8,2% em saúde, 7,5% em varejo ou atacado e 7% em educação. As demais possuem menores participações em atividades como mobilidade, entretenimento, turismo, agronegócios, *lawtechs* etc.

Como visto os números dos agentes de pequeno porte são expressivos e devem ser considerados sem titubeio na flexibilização da conformidade da legislação de proteção de dados.

Para tanto, observando o cenário externo, é possível identificar que a portabilidade de dados vem sendo discutida em outros países há alguns anos. Desse modo, é conveniente destacar a recente experiência da Comissão de Proteção de Dados Pessoais de Singapura[66], a qual realizou um estudo sobre os benefícios e questões que podem surgir com a introdução de um requisito de portabilidade de dados, incluindo o impacto sobre os consumidores, empresas e concorrência.

A partir desse estudo, discutiu-se alguns dos impactos da portabilidade de dados[67] em termos econômicos, os quais centraram-se principalmente em dois aspectos: (i) redução do custo de transferência de dados; e (ii) a capacidade de

---

[63] Disponível em: <https://datasebrae.com.br/totaldeempresas/>. Dados de maio, 2020. Acesso em 10 de fev. 2021.

[64] G1.Globo.com. Globonews. Número de startups no Brasio aumento 20 vezes nos últimos oito anos. 11 já são unicórnios. Disponível em: <https://g1.globo.com/globonews/noticia/2020/01/15/numero-de-startups-no-brasil-aumentou-20-vezes-nos-ultimos-oito-anos-11-ja-sao-unicornios.ghtml>. Acesso em 10 de fev.2021.

[65] O Momento da Startup Brasileira e o futuro do Ecossistema de Inovação. 2017. Mapeamento disponibilizado pela Abstartups em: <https://abstartups.com.br/radiografia-do-ecossistema/>. Acesso e download em 10 de fev.2021.

[66] PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE. **Discussion paper on Data Portability**. Singapura: Personal Data Protection Commission, 2019. Disponível em: https://bit.ly/3gVHFAR. Acesso em: 12 fev. 2021.

[67] Existem tensões potenciais entre os benefícios competitivos da portabilidade de dados e os aspectos de implementação da portabilidade de dados. Por exemplo, o impacto na redução dos custos de troca se o escopo da portabilidade de dados cobrir apenas uma faixa limitada de dados. Por outro lado, um direito oneroso de portabilidade de dados pode resultar em custos mais elevados para as empresas que implementam tal direito.

combinar dados de diferentes fontes. Como resultado disso, uma série de efeitos[68] podem ser identificados[69]:

(a) Efeitos sobre a concorrência no mercado decorrentes de custos de mudança potencialmente mais baixos e barreiras à entrada e expansão, onde os requisitos de portabilidade tornam mais fácil para os consumidores mudarem de prestadores de serviços e aumenta a capacidade de organizações novas ou existentes que dependem de dados como uma entrada importante para competir efetivamente respectivamente;

(b) Benefícios externos decorrentes do aumento do uso de dados, onde a portabilidade leva a mais dados sendo fornecidos por indivíduos às organizações, e isso pode gerar valor que não é (explicitamente) refletido no benefício recebido pelos próprios indivíduos;

(c) Maior produtividade derivada da facilidade de combinar dados de diferentes fontes, reduzindo assim o custo de produção de produtos e serviços habilitados para dados; e

(d) Inovação a partir da combinação de dados de novas maneiras em organizações e 'silos' da indústria.

Outrossim, no âmbito da União Europeia[70], o ponto crítico é como atender o direito do titular sem obstáculos, sem invadir a propriedade intelectual e causar risco aos segredos de negócio. Além disso, outro desafio é definir qual o real escopo dos dados pessoais sujeitos a portabilidade. Nesse sentido, somente os dados pessoais estritamente relacionado ao titular e requeridos devem ser transferidos. Por fim, as dificuldades técnicas que as micro e pequenas empresas têm para atender aos padrões de transferência de dados, sem riscos, como é o caso de startups.

Ademais, também em um recente estudo[71] publicado pela OCDE – "Organização para Economia Cooperação e Desenvolvimento", dentre outros assuntos, foi abordada a questão da portabilidade e interoperabilidade de dados. Concluiu-se que, a forma como os direitos e responsabilidades de portabilidade de dados são implementados tem implicações para resultados de competição.

A "portabilidade de dados prevista no GDPR impõe altos custos de conformidade", que quando aplicado a empresas não dominantes, pode impedir a concorrência e, em última análise, prejudicar os consumidores. Diante disso, é sugerido uma isenção (ou uma flexibilização) para pequenas e médias empresas e empresas com uma pequena participação de mercado ou volume de negócios.

---

[68]Dado que a portabilidade de dados não é amplamente implementada, esses efeitos principais dependem de uma série de suposições. Há pouca evidência empírica para a importância relativa de diferentes efeitos ou para o custo de implementação e conformidade. Estudos de mercado aprofundados são recomendados para identificar os efeitos e o provável equilíbrio de custos e benefícios para mercados ou setores específicos da economia.

[69] Os efeitos identificados neste documento de discussão podem diferir dependendo do tipo ou escopo dos dados que são transferidos ou combinados de fontes diferentes.

[70] EUROPEAN COMMISSION. Guidelines on the right to data portability. Disponivel em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>. Acessado em: 13 de fev. 2021.

[71] OCDE. Consumer Data Rights and Competition - Background note. Disponível em: <https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf>. Acessado em: 14 de fev. 2021

Voltando agora para o cenário brasileiro, o direito a portabilidade de dados pessoais está, embora de forma indireta, relacionado a necessidade dos agentes de pequeno porte, quando figurarem como controladores e ou operadores, se deverão ou não manter o registro das operações de tratamento dos dados pessoais que realizarem (artigo 37, LGPD).

De igual modo, o direito a portabilidade de dados também se relaciona com outros direitos e obrigações previstos na LGPD, tais como a necessidade da elaboração do relatório de impacto à proteção de dados pessoais; a nomeação do encarregado de dados; plano de governança; o acesso aos dados; a correção dos dados; a anonimização dos dados; a eliminação dos dados; e etc.

Portanto, o que se revela desde logo, é que o maior impacto para os agentes de pequeno porte para implementar a portabilidade de dados é o custo da conformidade. Pois, a sua implementação em grande parte, despende de alto investimento em tecnologia para a proteção dos dados. Além disso, outro enorme desafio é assegurar a interoperabilidade de dados.

Temos no setor bancário, como um ponta pé inicial, um possível caminho para auxiliar os agentes de pequeno porte à portabilidade de dados. O Banco Central no ano passado lançou o Open Banking, conforme a Resolução Conjunta n.º 1/2020[72], a qual dispõe o direito o compartilhamento de dados bancários. Para tanto, as instituições participantes devem disponibilizar interfaces dedicadas ao compartilhamento de dados e serviços, os quais devem ser representados em meio digital e processáveis por máquina, em formato livre de restrição quanto à sua utilização.

Nesse sentido, poderá a ANPD, em conjunto com a indústria de tecnologia, propor e viabilizar uma interface única, padronizada, segura, onde titulares de dados, controladores e operadores, possam requerer, dispor e transferir os seus dados pessoais.

Por fim, mas não menos importante, é fundamental estabelecer requisitos tais como a natureza da empresa, qual o seu porte, qual é o volume de dados tratados, para então estabelecer os critérios para flexibilização do direito a portabilidade de dados.

Tem-se que a portabilidade, isoladamente considerada, é um direito do titular, como quer a LGPD, e nenhum obstáculo pode lhe ser imposto para o pleno exercício deste direito.

Uma abordagem gradativa e proporcional, porém, sem menosprezar esse dever de adequação à Lei, deva então ser adotada pela ANPD em sua regulamentação.

Entre os critérios passíveis, vislumbra-se a adoção de escalas, em razão do porte das empresas ou agentes de tratamento de dados pessoais.

Estariam dispensados do dever de atender as solicitações de portabilidade de dados pessoais: a) os agentes pessoas físicas e b) as pessoas jurídicas classificadas como MEI ou EIRELI. Para os demais portes e classificações de agentes de

[72] BANCO CENTRAL DO BRASIL. Resolução Conjunta n.º 1/2020 BCB, 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf. Acessado em: 15 de fev. 2021.

tratamento e para qualquer porte de startups – com exceção às atividades também supervisionadas e reguladas por outras instituições reguladoras ou entidades de classe federal[73] -- a obrigação de atendimento às solicitações de portabilidade de dados realizadas pelos titulares seriam escalonadas em quantidade de titulares tratados e prazo para atendimento: a) empresas ou agentes com até 10.000 (dez mil) titulares – prazo de até 60 (sessenta) dias; b) empresas ou agentes entre 10.001 (dez mil e um) e 30.000 (trinta mil) titulares – prazo de até 45 (quarente e cinco) dias; c) empresas ou agentes entre 30.001 (trinta mil e um) e 50.000 (cinquenta mil) titulares – prazo de até 30 (trinta) dias; e d) empresas ou agentes com mais de 50.000 (cinquenta mil) titulares – prazo de até 15 (quinze) dias para atendimento.

Em qualquer das hipóteses, na inviabilidade do atendimento do requerimento de portabilidade, o controlador obrigatoriamente deverá enviar justificativas, de forma clara, transparente e objetiva acerca dos motivos que embasaram a decisão ou inviabilizaram o atendimento.

No caso de atividades supervisionadas ou reguladas também por demais instituições federais, como já comentado, a autoridade nacional deverá expedir os normativos em conjunto com referidas agências ou entidades reguladoras.

Sob a questão de alteração legislativa, o ponto a ser alterado na LGPD seria, então, no já citado artigo 18, inciso V:

(Nova redação) V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, e, no caso de atividades sujeitas a regulação de entidades ou instituições federais, regulamentação daquela em conjunto com estas. Em qualquer hipótese, serão observados e protegidos os segredos comercial e industrial, bem como os dados relacionados a terceiros.

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

Primeiramente, cabe observar que a ANPD poderá basear-se no art. 219-B da Constituição Federal, que traz relevantes diretrizes programáticas a serem observadas:

> Art. 219-B. O Sistema Nacional de Ciência, Tecnologia e Inovação (SNCTI) será organizado em regime de colaboração entre entes, tanto públicos quanto privados, com vistas a promover o desenvolvimento científico e tecnológico e a inovação
>
> § 1º Lei federal disporá sobre as normas gerais do SNCTI.
>
> § 2º Os Estados, o Distrito Federal e os Municípios legislarão concorrentemente sobre suas peculiaridades.

[73] Incluem-se o setor financeiro, energia, telecomunicações, medicina, saúde, advocacia, etc.

A formalização do “Sistema Nacional de Ciência, Tecnologia e Inovação (SNCTI)”, tem como característica o regime de colaboração entre entes públicos e privados, somente ocorreu mediante a incorporação do art. 219-B ao texto constitucional, por força da Emenda Constitucional 85, de 2015.

Outro instrumento que a Agência poderá basear-se é o Marco Regulatório da Inovação de 2016, a Lei nº 13.243/2016, que trouxe mais autonomia à Lei da Inovação de 2004.

A Lei nº 13.243/2016, Dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação e altera a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 6.815, de 19 de agosto de 1980, a Lei nº 8.666, de 21 de junho de 1993, a Lei nº 12.462, de 4 de agosto de 2011, a Lei nº 8.745, de 9 de dezembro de 1993, a Lei nº 8.958, de 20 de dezembro de 1994, a Lei nº 8.010, de 29 de março de 1990, a Lei nº 8.032, de 12 de abril de 1990, e a Lei nº 12.772, de 28 de dezembro de 2012, nos termos da Emenda Constitucional nº 85, de 26 de fevereiro de 2015.

A Lei da Inovação tem o objetivo de incentivar a parceria entre universidade, centros de pesquisa e as empresas. Para isso, são estabelecidos mecanismos que incentivam a cooperação para a produção científica, tecnológica e de inovação.

Sendo inspirada no modelo da Lei da Inovação francesa, a Lei nº 10.973/2004 é um marco para a inovação do Brasil. A lei baseia-se em três pilares: (i) construir um ambiente de parceria entre empresas e ICTs (Instituições Científicas e Tecnológicas); (ii) estimular a inovação por parte das ICTs (Instituições Científicas e Tecnológicas); (iii) estimular a inovação por parte das empresas privadas.

Quais são os impactos da lei da liberdade econômica nas atividades de agentes de pequeno porte?

A Lei da Liberdade Econômica (Lei nº 13.874/2019), já em seu artigo 1º declara que se destina a estabelecer “normas de proteção à livre iniciativa e ao livre exercício de atividade econômica e disposições sobre a atuação do Estado como agente normativo e regulador, nos termos do inciso IV do caput do art. 1º, do parágrafo único do art. 170 e do caput do art. 174 da Constituição Federal”.

Assim, como agente federal regulador, a autoridade nacional, a ANPD, também a ela se submete na concretização e complementação normativa da LGPD. Tanto é que, o Decreto nº 10.411, de 30 de junho de 2020[74], em seu artigo 3º, § 3º, não incluiu as normas regulamentares de caráter geral, como é o caso das regulamentações a serem expedidas pela ANPD, entre os casos de dispensa a AIR – Avaliação do Impacto Regulatório.

Logo, a Lei traz princípios em seu artigo 2º dispostos no sentido de nortear os agentes reguladores: I - a liberdade como uma garantia no exercício de atividades econômicas; II - a boa-fé do particular perante o poder público; III - a intervenção

[74] PLANALTO. Decreto nº 10.411, de 30 de junho de 2020. Regulamenta a análise de impacto regulatório. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10411.htm>. Acessado em 16 de fev. 2021.

subsidiária e excepcional do Estado sobre o exercício de atividades econômicas; e IV - o reconhecimento da vulnerabilidade do particular perante o Estado.

Também é relevante, quanto a essas balizas, trazer o que contempla o seu artigo 4º, caput e alguns dos seus incisos, em particular: Art. 4º - É dever da administração pública e das demais entidades que se vinculam a esta Lei, no exercício de regulamentação de norma pública pertencente à legislação sobre a qual esta Lei versa, exceto se em estrito cumprimento a previsão explícita em lei, evitar o abuso do poder regulatório de maneira a, indevidamente: I - criar reserva de mercado ao favorecer, na regulação, grupo econômico, ou profissional, em prejuízo dos demais concorrentes; II - redigir enunciados que impeçam a entrada de novos competidores nacionais ou estrangeiros no mercado; III - exigir especificação técnica que não seja necessária para atingir o fim desejado; IV - redigir enunciados que impeçam ou retardem a inovação e a adoção de novas tecnologias, processos ou modelos de negócios, ressalvadas as situações consideradas em regulamento como de alto risco; V - aumentar os custos de transação sem demonstração de benefícios; VI - criar demanda artificial ou compulsória de produto, serviço ou atividade profissional, inclusive de uso de cartórios, registros ou cadastros; VII - introduzir limites à livre formação de sociedades empresariais ou de atividades econômicas, como exemplo de alguns de seus incisos.

Percebe-se, ao avaliar-se estes preceitos legais, que a entidade reguladora, por meio da Avaliação do Impacto Regulatório, observando-se as diretrizes do Decreto nº 10.411, igualmente, deve adotar critérios razoáveis, fundamentados e os mais objetivos possíveis no cumprimento de suas atribuições.

As empresas de pequeno porte e as startups, como já analisado anteriormente, representam um potencial real de geração de emprego, além de desempenharem a função de possibilitar a inovação e a concorrência, evitando-se concentrações como quer os ditames constitucionais referidos, atuando em benefício dos consumidores, como resultado desse natural equilíbrio de forças.

Assim, o Estado Regulador, deve estar atento à essa importante missão no desempenho da atividade reguladora. Se por um lado a Lei impõe o dever de os reguladores fomentarem a concorrência, evitando-se a formação de grupos econômicos privilegiados, por outro lado, as disparidades técnicas e econômico-financeiras dos agentes de tratamento de dados de pequeno porte em relação aos demais agentes é gritante, e, portanto, reclamam um tratamento isonômico. Isonômico, no sentido da igualdade ou paridade material de armas ou condições[75], como postulou Rousseau para limitar os poderes arbitrários do Estado diante das desigualdades individuais, princípio que evoluiu em nosso mundo jurídico e encontra-se, por exemplo, insculpido no artigo 5º caput, segundo o qual “todos são iguais perante a lei”. No dizer de Canotilho, a ideia de igualdade inscrita nos vários textos constitucionais é a da igualdade material, pois, “a igualdade perante a lei é uma igualdade verificável na aplicação do direito, enquanto que, quanto à criação do direito (ou considerado o conteúdo da lei), a igualdade é no sentido de igualdade na própria lei”, ressalvando o citado autor que apenas se satisfaz a exigência constitucional por uma igualdade material[76].

[75] Para mais detalhes ver: <https://ambitojuridico.com.br/cadernos/direito-constitucional/o-principio-da-igualdade/.>. Acessado em 16 de fev. 2021.
[76] Idem, ibidem.

O Decreto nº 10.411/2020, em seu artigo 2º, II, “c”, afirma que é considerado ato normativo de baixo impacto aquele que não provoque aumento expressivo de custos para os agentes econômicos.

É nesse normativo que se fundamenta, em princípio, além de outras análises, a questão da dispensa de nomeação de Encarregado de Dados de que cuida o artigo 41, § 3º, da LGPD.

Também o artigo 6º, do referido Decreto, referindo à AIR, expõe metodologias, critérios técnicos e objetivos para padronizar o trabalho dos entes reguladores em seu ofício. Desse modo, por exemplo, citam-se os incisos: X – identificação e definição dos efeitos e riscos decorrentes da edição, alteração ou revogação do ato normativo; XI – comparação das alternativas consideradas para a resolução do problema regulatório; e XII – formas de monitoramento e de avaliação a serem adotadas, se se couber, avaliação quanto à necessidade de alteração ou revogação de normas vigentes.

Por outro lado, o artigo 7º, do Decreto, inclui entre as metodologias de aferição do impacto, os incisos II – análise de custo-benefício; IV – análise de custo; e V – análise de risco.

Finalmente, entende-se que a AIR é necessária na expedição das normas regulamentares e nas proposições de alterações legislativas, a serem levadas a cabo pela ANPD, considerando os princípios constitucionais de proteção das micro e pequenas empresas, do fomento à inovação e às atividades empresariais, do benefício aos consumidores que a concorrência leal pode trazer, sem deixar de atender ao necessário preceito, também constitucional, da defesa do consumidor, e os princípios de proteção da personalidade e da intimidade.

A LGPD, em seu encaminhamento regulamentar, há que ser interpretada e concretizada em sintonia – e de modo sistemático – com as demais legislações trazidas a colação neste Documento, de forma que as normas que diferenciem o tratamento a ser dado aos agentes de pequeno porte (pessoas físicas, empresas e startups), respeitem os parâmetros de aferição de justiça – como o da igualdade material, por exemplo – ao considerar os riscos potenciais e realmente esperados em suas atividades, segundo o porte e características, os custos e benefícios das exigências regulamentares e suas dispensas, os impactos na erosão de clientela que o exercício da portabilidade, como quer a LGPD, poderá ocasionar aos empresários vulneráveis e, como consequência, no normal desenvolvimento de suas atividades, com repercussões na geração de empregos e renda.

REFERÊNCIAS:

ARMERDING, Taylor. Why criminals pick on small business. 2015. Disponível em: https://www.csoonline.com/article/2866911/why-criminals-pick-on-small-business.html. Acesso em: 15 fev. 2021.

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR**. – 1. ed. – São Paulo: Thomson Reuters Brasil, 2020

BRASIL, Banco Central do. Resolução Conjunta n.º 1/2020 BCB, 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf. Acessado em: 15 de fev. 2021.

BRASIL, Ministério da Economia. Governo destaca papel da Micro e Pequena Empresa para a economia do país. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/outubro/governo-destaca-papel-da-micro-e-pequena-empresa-para-a-economia-do-pais. Acessado em 14 de fev. 2021.

BRASIL, República Federativa do. Lei Complementar nº 123, de 14 de dezembro de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm>. Acessado em 10 fev. de 2021.

_____. Lei Complementar nº 167, de 24 de abril de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp167.htm>. Acessado em 10 fev. de 2021.

_____.Lei 13.709, de 14.08.2018 (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em 10 fev. de 2021.

_____. Lei nº 13.874, de 20 de setembro de 2019 (Declaração de Direitos da Liberdade Econômica). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm>. Acessado em 10 fev. de 2021.

_____. Decreto nº 10.411, de 30 de junho de 2020. Regulamenta a análise de impacto regulatório. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10411.htm>. Acessado em 16 de fev. 2021.

CASTELLS, Manuel. **A Sociedade em Rede.** Trad. Roneide Venancio Majer, 21ª ed. São Paulo: Paz e Terra. 2020.

CAVOUKIAN, Ann. Operationalizing privacy by design: A guide to implementing strong privacy practices. Information and Privacy Commissioner, Ontario, Canada. 2012.

COMMITTEE ON SMALL BUSINESS. Small business, big threat: protecting small businesses from cyber attacks. 2015. Disponível em: https://www.congress.gov/event/114th-congress/house-event/LC30421/text?s=1&r=10. Acesso em: 15 fev. 2021.

EUROPEAN COMMISSION. Guidelines on the right to data portability.. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233. Acesso em: 13 de fev. 2021.

FREITAS, Cinthia Obladen de Almendra. **O que está em jogo no vazamento de milhões de CPFs?** ESTADÃO, 26 jan. 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/o-que-esta-em-jogo-no-vazamento-de-milhoes-de-cpfs/. Acesso em: 15 fev. 2021.

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2013. p. 02. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 15 jan. 2021.

ISO/IEC 27701. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. 2019. Disponível em: <https://www.iso.org/standard/71670.html>. Acesso em: 15 jan. 2021

MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados Pessoais. Manual de Implementação**. São Paulo: Thomson Reuters Brasil, 2019.

MAROSO, Eduardo Pereira *in*: **LGPD – LEI GERAL DE PROTEÇÃO DE DADOS: SUA EMPRESA ESTÁ PRONTA?** LIMA, Ana Paula Moraes de Canto et. ali. São Paulo: Literare Books International, 2020, p. 138.

MORALES-TRUJILLO, Miguel Ehécatl; GARCÍA-MIRELES, Gabriel Alberto; MATLA-CRUZ, Erick Orlando; PIATTINI, Mario. **A systematic mapping study of privacy by design in software engineering**, CLEI Electronic Journal, v. 22, n. 1, paper 4, April 2019. p.1-29.

OCDE. Consumer Data Rights and Competition - Background note. Disponível em: <https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf>. Acessado em: 14 de fev. 2021

PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE. **Discussion paper on Data Portability**. Singapura: Personal Data Protection Commission, 2019. Disponível em: https://bit.ly/3gVHFAR. Acesso em: 12 fev. 2021.

PONCE, Paula Pedigoni. Direito à portabilidade de dados: entre a proteção de dados e a concorrência. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/download/521/26/2041. Acesso em: 12 fev. 2021.

LINKS PESQUISADOS (acesso em 19 fev. 2021):

https://ico.org.uk/for-organisations/guide-to-data-protection/

https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/

https://exame.com/tecnologia/lei-de-dados-pessoais-muda-apps-porque-aperta-onde-doi-no-bolso/

https://jus.com.br/artigos/86483/pequenas-e-medias-empresas-e-a-adequacao-a-lei-geral-de-protecao-de-dados-do-brasil-aliada-as-boas-praticas-baseadas-na-general-data-protection-regulation-da-uniao-europeia

https://www.hipaajournal.com/small-businesses-gdpr-compliance/

https://www.i-scoop.eu/gdpr/gdpr-small-medium-businesses/

https://ec.europa.eu/justice/smedataprotect/index_pt.htm

https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais

https://www.billomat.com/pt/revista/rgpd-para-pequenas-empresas/

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527

https://migalhas.uol.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia

https://www.crowe.com/pt/insights/20200527-o-rgpd-e-as-pequenas-e-microempresas

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3123A0052&nid=3123&tabela=leis&pagina=1&ficha=1&so_miolo=?area=Identifica%E7%E3o%20civil%20e%20criminal&nversao=#artigo

https://www.phcsoftware.com/business-at-speed/rgpd-portugal-multas/

https://exame.com/pme/gdpr-nova-lei-europeia-de-dados-pessoais-ja-afeta-startups-brasileiras/

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

https://datasebrae.com.br/totaldeempresas/

https://g1.globo.com/globonews/noticia/2020/01/15/numero-de-startups-no-brasil-aumentou-20-vezes-nos-ultimos-oito-anos-11-ja-sao-unicornios.ghtml

https://abstartups.com.br/radiografia-do-ecossistema/

https://blog.privacyperfect.com/gdpr-for-smes-key-points>; <https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/>; e https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos

https://inplp.com/latest-news/article/the-estonian-data-protection-authority-issued-guidance-on-the-definition-of-large-scale-processing

https://ec.europa.eu/justice/smedataprotect/index_pt.htm

https://politica.estadao.com.br/blogs/fausto-macedo/o-que-esta-em-jogo-no-vazamento-de-milhoes-de-cpfs

http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf

https://www.iso.org/standard/39066.htm

https://www.iso.org/standard/54534.html

https://www.sis.se/api/document/preview/914169/

https://g1.globo.com/globonews/noticia/2020/01/15/numero-de-startups-no-brasil-aumentou-20-vezes-nos-ultimos-oito-anos-11-ja-sao-unicornios.ghtml

https://abstartups.com.br/radiografia-do-ecossistema/

https://ambitojuridico.com.br/cadernos/direito-constitucional/o-principio-da-igualdade/