CONTRIBUIÇÃO IBRAC À TOMADA DE SUBSÍDIOS Nº 1 /2021 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Introdução

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

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

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

Quais são os desafios/problemas regulatórios relacionados ao tema?

Um primeiro grande desafio relacionado ao tema é a **dificuldade de adequação de agentes de pequeno porte às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD).** Em vista da falta de conhecimento e familiaridade de agentes de menor porte sobre regras de proteção de dados, a **adequação de seus negócios à LGPD envolve custos financeiros diversos**, em decorrência da contratação de consultorias jurídicas e tecnológicas, contratação de softwares e tecnologias adequadas, contratação de profissionais especializados em LGPD para exercer o cargo de Encarregado e outros cargos correlatos, e ainda investimentos em monitoramento contínuo

de implementação da LGPD de todas as atividades de tratamento de dados e em treinamento de seus profissionais1[1]. De acordo com Relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento ("UNCTAD") a respeito do impacto das regulamentações de proteção de dados no comércio[2], a aprovação dessas normas pode colocar empresas de pequeno porte em desvantagem competitiva e criar obstáculos (ônus de compliance regulatório) que poderão incentivar sua saída do mercado, o que, por sua vez, acabaria por desestimular a inovação, reduzir as escolhas do consumidor e aumentar o risco de monopolização por grandes empresas já estabelecidas no mercado.

Como contorno a esses problemas, a flexibilização das normas para esses agentes pode ser considerada uma resposta para garantir a redução dos custos e, assim, não frear a competitividade e inovação no mercado. No entanto, outro desafio surge: **uma flexibilização excessiva de obrigações regulatórias pode também acarretar riscos para a proteção dos direitos de titular de dados, desvirtuando-se das diretrizes da própria LGPD.** Ilustra-se esse problema o fato de existirem agentes econômicos de pequeno porte dedicados à exploração intensiva de dados associados a um número significativo de titulares, que poderiam então, estar sujeitos à uma regulação flexibilizada de forma desproporcional. Sendo assim, é necessário, ao desenhar uma regulação específica aos agentes de pequeno porte, levar em conta um equilíbrio ideal os custos envolvidos para o atendimento de tal regulação e os possíveis problemas para a dinâmica empresarial de diferentes tipos de empresas. A regulação deve ser estruturada de modo que pequenas

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

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

empresas a vejam como suficientemente legítima e que seus benefícios superem os custos relacionados a seu cumprimento. [3]

Ainda, exigências e responsabilidades em face do titular podem variar muito a depender do tipo de agente de pequeno porte e o núcleo de suas atividades, como quando comparamos, por exemplo, um pequeno ponto de venda de bebidas (em que os dados pessoais envolvidos podem consistir apenas nos dos funcionários do local) ou um administrador de banco de dados (o qual pode atuar como operador para grandes empresas que realizam o tratamento de dados sensíveis). **Em vista da diversidade não uniforme de tipos de agentes e suas estruturas com relação ao tratamento de dados pessoais, também surge o desafio da autoridade em desenvolver o endereçamento de uma regulação adequada a cada tipo específico**, de modo que não se desvie da finalidade esculpida pelo art. 55-J, XVIII, da LGPD, que é a criação de uma regulação adaptada às situações em que não seria ideal – e até mesmo prejudicial – aos agentes econômicos previstos no dispositivo a atenderem de maneira inflexível todos os requisitos contidos na LGPD.

Outro grande desafio é o de que as **exigências regulatórias cheguem ao conhecimento, de maneira clara e objetiva aos agentes de pequeno porte para que possam entrar em conformidade sem que sejam impedidos pelo desconhecimento de termos técnicos**. Além disso, é preciso considerar também a dificuldade de inserir determinadas práticas com relação à proteção e privacidade de dados dentro do ambiente cultural e rotina dos agentes de pequeno porte. Nesse sentido, para além de uma adequação de uma regulação multisetorial, é necessário um forte trabalho institucional e comunicacional para dispersão de informação e conhecimento afetos ao tema da proteção de dados, de maneira simples, clara e objetiva, modos de adequação e exigências e a relevância em si da proteção de dados e sua incorporação na empresa, bem como eventuais consequências por não conformidade.

Por fim, ainda reside o desafio de **comportar na regulamentação sobre o tema as operações de tratamento de dados relativos ao desempenho de atividade econômica por pessoas físicas e entidades não-empresariais.** Quanto à primeira categoria, ao considerarmos o quadro da

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

economia brasileira, marcada pela informalidade[4], cumulada aos diversos modelos de negócios desenvolvidos por profissionais liberais, o tratamento de dados pessoais por pessoas físicas para fins econômicos passa a ser relevante. Tal constatação também é observada nos casos de entidades não-empresariais, tal como organizações não-governamentais e associações, que podem também realizar atividades de tratamento de dados pessoais em menor ou maior escala. Estes sujeitos, em vista de suas características, também devem enfrentar dificuldades na adequação de seus negócios à LGPD, seja pela falta de recursos financeiros ou pela falta de conhecimento e familiaridade sobre regras de proteção de dados. Da mesma forma que citado anteriormente, algumas exigências podem ser irrazoáveis para garantir a proteção de dados buscada pela lei, em vista das diferentes estruturas de cada agente. Nesse sentido, entendemos que a isonomia de tratamento entre pessoas físicas que manipulam dados para fins econômicos bem como entidades não-empresariais de menor porte, e agentes de pequeno porte, merece ser considerada.

Existem sugestões para endereçamento do problema?

Sim. Uma primeira sugestão, seria garantir que a LGPD seja aplicada, ao menos, de maneira diferenciada e mitigada para esses pequenos empresários e empresas de pequeno porte, ou, mesmo prevendo isenções a essas categorias de empresas e profissionais, de forma a adequar ou mesmo reduzir seu ônus de adequação regulatória. Para regular adequadamente a atuação desses atores, um primeiro passo seria incluir critérios para sua definição como agentes de pequeno porte. Atualmente, empresas de menor porte são classificadas como tal a partir do seu faturamento anual, conforme definição de da Lei Complementar 123/2006. Este critério de definição sozinho para justificar a flexibilização de normas, no entanto, não parece adequado. Como agentes de menor porte podem possuir atividades de tratamento de dados em maior escala e/ou mais arriscadas que agentes de maior porte, a adaptação de normas para agentes a partir de uma classificação baseada em faturamento, poderia implicar em regras desproporcionais para agentes com atividades de tratamento com potencial maior de risco. Nesse sentido, entendemos que a autoridade poderia optar por (i) seguir a definição

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

de micro e pequenas empresas da Lei Complementar 123/2006 e, em seguida (ii) estabelecer critérios secundários, cumulativos, para a definição dos agentes, baseados nas características das atividades de tratamento de dados desempenhadas.

Ainda, conforme pesquisa realizada em 60 empresas de pequeno porte em diferentes países europeus, em parceria com a União Europeia no âmbito do Programa 2014-2020 de Direitos, Equidade e Cidadania[5], foi possível constatar que os agentes privilegiam a acessibilidade e transparência de autoridades supervisoras no processo de auxílio de adequação dos agentes à regulação, em especial por entenderem que, salvo raras exceções, empresas do mesmo porte não possuem conhecimento interno extensivo sobre o regramento de proteção de dados. Nesse sentido, para que o ônus de adequação de tais agentes não seja demasiado custoso, experiências internacionais apontam para a formulação de guias e orientações públicas, publicadas como manuais, cadernos, panfletos, infográficos, etc., que podem ser inclusive direcionadas a determinados setores, facilitando a compreensão para agentes de determinado ramo. Por meio dessas publicações institucionais é facilitada a difusão de informações em linguagem menos técnica, de modo a facilitar a familiarização com o tema para os agentes e levantar a importância de conformidade com a legislação de proteção de dados. Isso pois a educação relacionada ao tema deve ser feita de tal forma que se reduza a percepção de complexidade, aumente a legitimidade da regulação e denote os custos e consequências envolvidas no seu cumprimento. Dessa forma, também se enquadram nessas sugestões a implementação e difusão de campanhas de conscientização que se mostram relevantes para aumento da capilaridade da regulação.

Nesse sentido, podem ser realizadas, além dos mecanismos de consulta pública, a realização de pesquisas específicas sobre o tema para avaliação dos diversos agentes e suas percepções e necessidades ou checagem do nível de conformidade existente. Um ponto importante também é a manutenção de canais de contato com associações, organizações ou entidades representativas de determinados setores de modo a facilitar a abordagem e análise de questões ou problemas existentes e que eventualmente podem decorrer de uma nova regulação e procedimentos. Além disso, poderiam ser oferecidos canais de atendimento (*hot desks*) facilitados e eficientes para o

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

atendimento de dúvidas relacionadas às eventuais exigências diferenciadas pela autoridade em caso de dúvidas. Para temas mais complexos, também poderiam ser previstos mecanismos de consulta administrativa que teriam valor de imunização no que tange à questão e à sugestão decidida.

Por fim, como desenvolvido no último tópico de contribuição, a implementação de *sandboxes* regulatórios com a flexibilização das normas em espaços controlados poderia contribuir para promoção de projetos de inovação por empresas de pequeno porte e startups, bem como para adequar dificuldades em detrimento da multiplicidade de setores, com exigências de regulações dinâmicas. Tal instrumento regulatório vem sendo utilizado principalmente em segmentos dos mercados de capitais e financeiro em diversos países. Porém, deve-se ter em conta que é preciso observar os limites legais e de competência para o estabelecimento lícito de sandboxes regulatórias. Outras sugestões importantes nesse sentido, considerando a ideia de flexibilidade e atenuação dos impactos regulatórios sentidos pelos agentes, podem ser a oportunidade de menus regulatórios, com a possibilidade de escolha de regras mandatórias alternativas, e *grandfathering*, consistente em regimes transitórios graduais para as novas estatuídas. Além disso, poderiam ser oferecidos selos e certificações especiais para determinados casos como modo de comprovar conformidade com a lei e regulamentos de modo a aumentar a credibilidade perante terceiros e incentivar a adequação às normas, como prevista na GDPR.

Quais são as oportunidades relacionadas ao tema?

Os ganhos com a regulamentação dos agentes de pequeno porte são diversos. Em primeiro lugar, sua regulamentação, garantindo a adequação de normas para agentes de pequeno porte (originalmente pensadas para grandes processadores de dados), oferece melhores condições para um *level playing field* entre esses agentes e demais empresas. Em segundo lugar, a redução de ônus regulatórios excessivamente onerosos impostos a agentes de pequeno porte contribui para a criação de um ambiente regulatório que fomente a inovação tecnológica, um dos fundamentos da disciplina de proteção de dados inaugurada com a LGPD[6].

[6] Lei Geral de Proteção de Dados, Art. 2º:

"A disciplina da proteção de dados pessoais tem como fundamentos:

(...) V – o desenvolvimento econômico e tecnológico e a inovação;"

Outra oportunidade decorrente da regulamentação do tema é a possibilidade de estabelecer um padrão institucional de relacionamento e comunicação, que poderá facilitar a interação entre os diferentes agentes com a autoridade. Ainda, com uma abordagem adequada da regulamentação, seria possível a difusão de um padrão cultural de maior informação, familiaridade e respeito à temática relacionada a proteção de dados pessoais, principalmente direcionada a agentes que talvez não sejam tão afetos ao assunto. Por esse lado, haveria ao mesmo tempo um incremento na proteção dos direitos dos titulares de dados pessoais e uma imunização de determinados agentes com relação ao revés relacionado às aplicações de sanções relativas ao não cumprimento ou violação da legislação de dados pessoais, como multas que podem significar valores importantes e cruciais para agentes de pequeno porte. Ademais, o tema pode ser aproveitado para o desenvolvimento de relações baseadas na transparência e na proteção de dados pessoais entre clientes, empresas, consumidores e parceiros comerciais.

Por fim, o aproveitamento de maior simetria regulatória com experiências internacionais de regulação que já demonstraram sucesso – em especial na União Europeia, que possui legislação similar à brasileira -, garante maior segurança jurídica nas transferências internacionais de dados decorrentes de contratos entre agentes de pequenos portes e fornecedores estrangeiros. De outro lado, o aproveitamento de experiências internacionais também contribui para que a autoridade evite desenhar soluções inadequadas do ponto de vista de políticas públicas de proteção de dados, pela constatação de iniciativas ineficientes desenvolvidas por outras autoridades.

Quais são as experiências internacionais sobre o tema?

Ao observar experiências internacionais sobre o tema, é possível dividi-las em dois níveis: a atuação de países, a partir de sua regulamentação, inclui uma flexibilização total de normas de proteção de dados completa para agentes de pequeno porte, ou, importam em uma flexibilização parcial.

No primeiro caso, tem-se regulações que concedem isenções a empresas que estejam abaixo de um determinado limite. A Austrália, por exemplo, a partir do Ato de Privacidade de 1988 (“APA”) isenta pequenas empresas e organizações sem fins lucrativos que possuem faturamento anual de $ 3.000.000 (três milhões de dólares australianos) ou menos[7]. Tal isenção,

[7] AUSTRALIA, Privacy Act. 1988. Seção 6D. Disponível em: < https://www.legislation.gov.au/Series/C2004A03712 > Acesso em 18/02/2021.

no entanto, não será aplicada para pessoas ou entidades que comercializam informações pessoais, provedores de serviços de saúde, e agências de relatórios de crédito ou agentes que de outra forma lidam com informações financeiras críticas. O APA também oferece um mecanismo de "*opt-in*" para pequenas empresas que receberam essa isenção, para que, voluntariamente, se tornem sujeitas às regras do Ato da mesma forma que uma entidade coberta diretamente pela normativa, com vistas a demonstrar ao mercado e consumidor sua conformidade com o regramento de proteção de dados. Ou seja, seria um mecanismo de adesão voluntária à legislação por aqueles que, mesmo elegíveis à isenção regulatória, veem maiores benefícios na adequação plena de seu negócio ao regime protetivo de privacidade. Além disso, mesmo aceitando voluntariamente a incidência da norma aos seus negócios, esses agentes econômicos podem, posteriormente, notificar sua retirada[8], ampliando o leque de alternativas para lidar com os excessivos ônus regulatórios da legislação de proteção de dados.

Da mesma forma, a Lei de Privacidade do Consumidor da Califórnia de 2018 ("CCPA") é aplicável apenas a empresas cuja receita anual exceda US$ 25.000.000,00 (vinte e cinco milhões de dólares americanos), ou cuja metade da receita anual seja obtida com a venda de informações pessoais de consumidores ou que processem informações pessoais de pelo menos 50.000 pessoas anualmente[9]. Vale ressaltar, no entanto, que o último critério é objeto de diversas críticas por implicar em limiar demasiado baixo - e por consequência ampliar o universo de empresas sujeitas ao regime protetivo - visto que é razoavelmente fácil atingir o patamar de 50.000 pessoas/ano[10].

Nesse critério baseado em volume de dados ou titulares potencialmente afetados, o Japão, por exemplo, optou por abandonar a isenção conferida a entidades que não tratam informações pessoais de mais de 5.000 indivíduos em qualquer dia nos últimos seis meses. Cumpre mencionar, porém, que a legislação de proteção de dados japonesa permite que isenções sejam fornecidas em uma análise casuística, por meio de decisões nos casos

---

[8] *Ibid*. Seção 6EA.

[9] ESTADOS UNIDOS DA AMÉRICA, California Consumer Privacy Act. 2018. Seções 1798.100 a 1798.199 e Seção 1798.140(c). Disponível em: < https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121&showamends=false > Acesso em 18/02/2021

[10] Ver: COMSTOCK, Brendon. How the CCPA could be great for startups. 2018. Disponível em: < https://iapp.org/news/a/how-the-ccpa-could-be-great-for-startups/ > Acesso em 18/02/2021

em que o risco de danos aos direitos e interesses dos indivíduos se mostre limitado[11].

Do outro lado, o Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") recomenda que os Estados membros levem em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do regulamento[12], se aproximando de um modelo por isenções parciais. Em primeiro lugar, o GDPR isenta empresas com menos de 250 funcionários da obrigação de manutenção de registros de atividade de tratamento de dados, contanto que o tratamento de dados não seja ocasional, não resulte em riscos à liberdade de indivíduos e/ou não envolva determinadas categorias como dados pessoais sensíveis ou condenação criminal. além de trazer exceções à obrigação de nomeação de *Data Protection Officer* ("DPO"), cuja figura equivalente na legislação brasileira seria o Encarregado.

Vale ressaltar que, a implementação de exceções e flexibilizações normativas para agentes de menor porte em regramentos de proteção de dados pessoais não necessariamente reduzirá a dificuldade de adequação pelos agentes. No caso da União Europeia, segundo pesquisa[13] realizada pelo GDPR.EU, os principais pontos problemáticos relacionados à adequação das pequenas empresas[14] na Espanha, Reino Unido, França e Irlanda ao GDPR são: (i) aproximadamente metade das empresas estavam falhando em cumprir requisitos essenciais de linguagem clara sobre o tratamento aos titulares e identificação de base legal; (ii) confusão com conceitos básicos de segurança de dados; (iii) realização de investimentos em tecnologia e consultas para adequação; e (iv) reconhecimento majoritário da importância de conformidade à legislação.

---

[11] JAPÃO, Ato de Proteção de Dados Pessoais, Artigo 2º, Capítulo IV, Seção 1. Disponível em: < https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf > Acesso em 18/02/2021.

[12] UNIÃO EUROPEIA, General Data Protection Regulation, Recital (98), (132) e (167); Seção 5, Artigo 40. Disponível em: < https://gdpr-info.eu/ > Acesso em 18/02/2021.

[13] 2019 GDPR Small Business Survey. Disponível em: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf

[14] A definição da pesquisa é a de que pequenas empresas possuem menos de 500 empregados. Entretanto a categoria legislativa europeia de define como médias-empresas até 250 pessoas, considerando o enquadramento econômico. De qualquer modo consideramos possível extrapolar, ainda que grosseiramente, o resultado da pesquisa para agentes de pequeno porte.

De forma mais geral, foi observado[15] que as principais impressões de pequenas empresas na União Europeia no que tange à adaptação legal foram: custos consideráveis para adaptação, dificuldade no atendimento de direitos dos titulares em razão da falta de ferramentas adequadas, relativa dificuldade na implementação do princípio de prestação de contas pelo aumento de recursos humanos e custos financeiros, falta de derrogações adequadas a esse tipo empresarial, importância dos códigos de condutas para cumprimento da legislação, elevados custos relativos à certificação, reconhecimento do valor de guias e ferramentas práticas disponibilizadas, fardo com aumento da documentação, alto custos na elaboração relatório de impactos a proteção de dados pessoais, diminuição de custos de transação a partir de cláusulas contratuais padrão.

Nesse sentido, algumas autoridades nacionais buscam remediar essas dificuldades oferecendo guias e suporte prático de orientação e adequação à legislação de proteção de dados, nesse sentido se destacando a autoridade francesa[16], a autoridade irlandesa[17] e autoridade do Reino Unido[18]. Além disso, são também praticadas campanhas de conscientização voltadas a pequenas empresas para que tomem conhecimento sobre a legislação de proteção de dados e auxiliar esses agentes no cumprimento de suas obrigações legais[19]. Dessa forma, as autoridades vêm prezando pela conscientização e facilitação às pequenas empresas por meio de guias, ferramentas (como contratos padrões e registros de atividades), FAQs, canais de atendimento, campanhas e linhas de apoio. A União Europeia, de forma centralizada a partir

---

[15] Contribution From The Multistakeholder Expert Group To The Stock-Taking Exercise Of June 2019 On One Year Of Gdpr Application. 13 junho de2019. Disponível em:

https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf

[16] Guia disponível em: https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.

[17] Guia e orientação disponíveis em: https://www.dataprotection.ie/en/dpc-guidance/guidance-smes

[18] Em seu site, a ICO disponibiliza uma série de informações, orientações e ferramentas para pequenas empresas com relação à proteção de dados pessoais: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/

[19] GDPRights: GDPR awareness campaign and support to business organisations, in particular, SMEs. Disponível em: https://idpc.org.mt/idpc-publications/gdpr-awareness-campaign-business-organisations-in-particular-smes/https://idpc.org.mt/idpc-publications/gdpr-awareness-campaign-business-organisations-in-particular-smes/

do sítio ec.europa.du, também já publicou informativos para auxiliar pequenas empresas na adequação ao GDPR.[20]

No Reino Unido, por exemplo, o *Information Commisioner's Office* (ICO) visualiza a possibilidade de realização de um *sandbox* regulatória para casos de tratamento de dados pessoais, realizando uma consulta pública para visualização das dificuldades para inovação relacionadas ao tema da proteção de dados, qual seria o escopo de aplicação da *sandbox* regulatória, seus benefícios e mecanismos de funcionamento.[21] Em geral, houve um feedback positivo para o desenvolvimento de tal instrumento regulatório, mas a autoridade consignou que este deveria estar limitado a produtos e serviços que representem inovação genuína, que demonstrem benefícios materiais aos titulares de dados e que possuem uma estrutura de prestação de contas robusta para o tratamento de dados pessoais.

Por fim, vale ressaltar ainda a dificuldade observada em experiências internacionais quanto à convergência de regulamentos setoriais com regras de proteção de dados. A exemplo, no setor agrícola, perspectivas antagônicas às premissas do GDPR foram adotadas na União Europeia para o tratamento de determinadas informações do setor agrícola (e de outros setores econômicos) com a edição do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia[22]

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

Partindo de disposições já existentes no ordenamento jurídico brasileiro (Lei Complementar nº 123/2006, art. 1º, §§ 3º e 6º; Constituição Federal, arts. 146, "d", 170, IX, e 179; Lei nº 13.874/2019, art. 4º), nota-se que há autorização legal para criação de regimes especiais simplificados para microempresas e empresas de pequeno porte. Há, também, definições de "startups", "microempresas" e "empresas de pequeno porte" em normas

[20] Documento disponível em: https://ec.europa.eu/justice/smedataprotect/index_en.htm.

[21] O resumo da análise dos comentários da ICO está disponível em: https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf

[22] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1807.

vigentes ou avançadas no processo legislativo que podem ser consideradas pela autoridade, com o objetivo de uniformização do ordenamento jurídico e garantia de segurança jurídica na aplicação das normas.

Não obstante, a definição de um *proxy* preciso para definição de agentes de pequeno encontra dificuldades tanto em termos quantitativos quanto em termos qualitativos, pois deve considerar os diferentes tipos de agentes envolvidos, suas intersecções e os riscos relacionados. A utilização apenas de fatores quantitativos (como número de funcionários, receita anual, valor dos ativos, volume de dados) pode ser um problema, pois esses números podem muitas vezes não refletir os riscos aos direitos dos titulares e suas possíveis violações. Ademais, a consideração de valores qualitativos pode trazer problemas de enquadramento de determinados agentes como agentes de pequeno porte quando em comparação com critérios quantitativos mais objetivos, além de que apesar de endereçarem as questões de risco de modo mais adequado, podem não refletir o risco factual na realidade de determinado a gente quando levada de maneira isolada. Assim, os critérios devem ser conjugados de modo a trazer uma definição mais correta de agentes de pequeno porte.

Nesse sentido, experiências internacionais podem contribuir para a definição de critérios que se mostrem mais razoáveis para um ideal equilíbrio entre os fundamentos da disciplina de proteção de dados previstos na LGPD. A União Europeia, por exemplo, utiliza como critério para necessidade de designação de Encarregado a (i) existência de tratamento de dados como parte de atividades essenciais e não auxiliares da empresa e (ii) a existência de tratamento em larga escala. Similarmente fez a autoridade de proteção de dados australiana, que isenta da aplicação de obrigações de sua legislação de proteção de dados pequenas empresas com base no seu faturamento, ainda que tal isenção não seja aplicada para agentes que comercializam informações pessoais, sejam provedores de serviços de saúde, ou sejam agências de relatórios de crédito ou agentes que de outra forma lidem com informações financeiras críticas.

Em suma, entendemos que a ANPD poderia se valer dos critérios já estabelecidos em leis existentes ou em discussão legislativa no Brasil como ponto de partida para a definição de agentes de pequeno porte, garantindo, contudo, flexibilização e adaptação de obrigações para aqueles que se enquadrarem na classificação da lei, ainda que, permita exceções para a classificação dos agentes, a depender da vulnerabilidade dos dados tratados em suas atividades de tratamento, o volume de dados tratados, a existência de

atividades de tratamento essenciais ao negócio, entre outros critérios secundários.

Vale pontuar que o conceito de agentes de tratamento de dados de pequeno porte deve abranger as pessoas físicas que desempenham atividades econômicas de maneira desvinculada de pessoas jurídicas. Ademais, entendemos ser recomendável a criação de dois "blocos" de definição e regulamentação específica: PMEs, pessoas físicas e microempresas, de um lado, e startups, de outro, a fim de que sejam respeitadas as particularidades desta figura.

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

Para além das regras de isenção parcial prescritas no GDPR, a União Europeia divulga material informativo prático para auxiliar e conscientizar pequenas empresas sobre a importância de adaptação às novas regras legais existentes.[23]-[24] Além disso, há incentivos a campanhas de conscientização e ações de sensibilização nos níveis europeu e nacional através do financiamento, podendo ser citadas as experiências nacionais de campanhas de conscientização da Bélgica, Dinamarca, Holanda, Eslovênia, Islândia, Letônia, bem como a criação de ferramenta inovadora para pequenas empresas da Bulgária e materiais de treinamento direcionados a esse perfil pela Hungria.[25]

Como ações futuras dentro desse tema, o bloco europeu ainda prevê "desenvolver instrumentos práticos, tais como formulários harmonizados para as violações de dados e os registros simplificados das atividades de tratamento, para ajudar as PME de baixo risco a cumprirem as suas obrigações" e "apoiar as atividades das autoridades de proteção de dados que facilitem a aplicação das obrigações decorrentes do RGPD pelas PME, através

[23] Seven steps for businesses to get ready for the General Data Protection. Disponível em: https://ec.europa.eu/info/sites/info/files/gdpr2019-smes_7_steps_brochure-en-v03_lr_qc.pdf

[24] Better rules for small business. Disponível em: https://ec.europa.eu/justice/smedataprotect/index_en.htm

[25] Informação e mais detalhes disponíveis em: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

de apoio financeiro, especialmente para orientações práticas e ferramentas digitais que possam ser reproduzidas noutros Estados-Membros".[26]

Vale notar que a Agência de Cibersegurança da União Europeia (ENISA), já se manifestou preocupada com a adequação de empresas de pequeno e médio porte, ao publicar Guia de Segurança em Sistemas de Computação em Nuvem para Empresas de Pequeno e Médio Porte[27] e Guias sobre Segurança em Tratamento de Dados Pessoais por Empresas de Pequeno e Médio Porte[28], recursos estes, importantes para atender a requerimentos técnicos de segurança exigidos pelo GDPR.

Ainda, com base em levantamento feito em setembro de 2020 por projeto de pesquisa da União Europeia no âmbito do Programa 2014-2020 de Direitos, Equidade e Cidadania[29], pouco menos de um terço das autoridades de proteção de dados europeias oferecem orientações direcionadas especificamente para empresas de pequeno e médio porte. Daquelas que realizam, vale ressaltar, principalmente, a atuação das autoridades nacionais inglesa, ICO, (até início de 2020, pertencente à UE) e eslovena, IP. Quanto à autoridade inglesa, medida interessante implementada pela entidade foi segmentar o atendimento a empresas de menor porte em relação àquelas de grande porte, a partir de um canal telefônico específico para atender às dúvidas e demandas de pequenas empresas. Em sua plataforma online, a autoridade também disponibiliza FAQs, checklists para avaliar grau de adequação ao GDPR, templates para políticas de privacidade, to-do lists para respostas de incidentes de segurança, entre outros instrumentos em linguagem facilitada e

---

[26] Comissão Europeia. Comunicação (2020), 264: A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital - dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0264&from=EN#footnoteref49.

[27] Disponível em: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

[28] Disponíveis em: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/march-2015/presentations/presentation-nlos-cgm-v2.pdf e https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

[29] JASMONTAITĖ-ZANIEWICZ, Lina et al. The GDPR made simple(r) for SMEs. 2021. p. 24. Disponível em: <https://library.oapen.org/bitstream/handle/20.500.12657/46614/Handboek_GDPR_ENG_HR-cert-febr4.pdf?sequence=1> Acesso em 16/02/2021.

direta para facilitar o atendimento do GDPR por agentes de pequeno porte[30]. A autoridade eslovena, por sua vez, possui uma plataforma específica direcionada somente a empresas de pequeno e médio porte, onde estas podem acessar FAQs e formulários para designação de encarregado, para notificação de incidentes à autoridade, para notificar titulares sobre a obtenção de seus dados, bem como formulários para registro de atividades de tratamento de dados (adaptadas para controladores e operadores), em atenção à exigência de registro de atividades de tratamento prevista no GDPR (Art. 30)[31]. A autoridade também ofereceu um canal telefônico de auxílio a empresas de pequeno e médio porte durante um ano após a entrada em vigor do GDPR.

Demais autoridades também apresentam iniciativas destinadas a auxiliar empresas de pequeno porte. A autoridade belga (APD), também possui guias de adequação ao GDPR, FAQs e campanhas de conscientização destinadas a agentes de pequeno e médio porte. A autoridade francesa[32] (CNIL) e a lituana[33] (VDAI) também possuem guias com linguagem simplificada para adequação ao GDPR de empresas de micro, pequena e médio porte. No mesmo sentido, a autoridade irlandesa também dispõe em sua plataforma online guia de adequação destinado a empresas de pequeno e médio porte, incluindo checklists de adequação e templates para mapeamento de atividades de tratamento atuais das empresas[34]. A autoridade espanhola (AEPD), por sua vez, conta com ferramenta em sua plataforma online destinada a auxiliar a adequação de empresas que realizam tratamento de dados pessoais que implicam em riscos menores (que podem abranger o caso de diversos agentes de pequeno porte), conforme seu setor de atuação[35].

Por fim, há expectativa de se tornar a linguagem acessível, prática e menos técnica, garantindo que os agentes possam entender as orientações com

---

[30] Disponível em: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/

[31] Disponível em: https://upravljavec.si/vprasalnik/

[32] Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf

[33] Disponível em: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_SVV_BDAR_2018.pdf

[34] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf

[35] Disponível em: https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

menor dificuldade[36]. E em caso de infração às normas de proteção de dados, a União Europeia adota uma linha de imposição gradual de penalidades. Inicialmente é feito um aviso, seguido de advertência, suspensão e, em casos mais graves, até mesmo multas de até 20 milhões de euros ou 4% da receita anual global.

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

A depender da organização, a manutenção de registro das operações de tratamento de dados pode representar um custo elevado, tanto financeiro quanto administrativo. A título de exemplo, volumes excessivos de dados podem aumentar os custos de armazenagem de informação. A experiência europeia, nesse sentido, aponta para esse relevante impacto e para a dificuldade de adequação à GDPR por pequenos empresários e empresas de pequeno porte[37].

Contudo, o registro de operações de tratamento de dados pessoais auxilia no cumprimento da transparência e da prestação de contas perante terceiros e autoridades. Resumidamente, trata-se de um mecanismo importante para apoiar uma análise de riscos de qualquer atividade de tratamento existente em uma empresa. Sua manutenção facilita a avaliação factual do risco das atividades de tratamento realizadas por um controlador ou operador sobre os direitos dos indivíduos, e a identificação e implementação de medidas de segurança adequadas para salvaguardar os dados pessoais - ambos componentes essenciais do princípio de responsabilidade contido na LGPD.

Por esse motivo, um modelo mais flexível, como o desenvolvido pela GDPR, pode ser mais adequado para agentes de pequeno porte que não representem riscos demasiados a direitos dos titulares.

Atualmente, a LGPD estabelece que o registro é obrigatório para todas as atividades de tratamento, não possuindo exceções, seja para categorias de agentes sujeitos à norma, seja para atividades específicas de

---

[36] BARNARD-WILLS, David, et. al. Report on the SME experience of the GDPR. 2019. p. 31 Disponível em: <https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf> Acesso em 19/02/2021.

[37] Ver: https://gdpr.eu/2019-small-business-survey/ e https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf.

tratamento. Ademais, a lei não prescreve modelo de registro que possa ser implementado pelas empresas com segurança, as quais correm o risco de receber questionamento por omissões em registros pela autoridade nacional no futuro, em vista da falta de orientação. Desta forma, em linha com o entendimento do *Working Party* 29 sobre o registro de atividades de tratamento por empresas de micro, pequeno e médio porte[38], recomenda-se que a ANPD forneça ferramentas para facilitar a criação e gestão de registro. Por exemplo, poderia ser disponibilizado no sítio da ANPD na Internet, um modelo simplificado que pode ser utilizado pelos agentes para manter registros das atividades.

Ademais, a autoridade poderia estabelecer um prazo de armazenagem de dados diferenciado para empresas de menor porte, bem como se valer de derrogações implementadas pela União Europeia em relação à obrigação de registro de atividades de tratamento prevista no GDPR. Conforme o art. 30 do Regulamento europeu, o registro de atividades de tratamento por empresas ou organizações que empreguem menos de 250 pessoas pode ser dispensado, a não ser que o tratamento de dados conduzido pela pessoa jurídica possa resultar em risco aos direitos e liberdades de titulares de dados, seja ocasional ou o tratamento inclua dados sensíveis ou dados relacionados a ofensas e condenações criminais. Entendemos que exceções similares poderiam ser implementadas para agentes de pequeno porte no Brasil.

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

Entre os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte está o alto custo a ser despendido neste trâmite. Vale lembrar, os agentes de pequeno porte não possuem tantos recursos para realizar tal nomeação. Desta forma, seria relevante o aproveitamento dos critérios presentes na GDPR sobre a flexibilização da exigência de encarregado para os agentes de pequeno porte.

[38] WORKING PARTY 29, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR. Disponível em: <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422> Acesso em 18/02/2021.

Na GDPR, a designação de encarregado é dispensada para os agentes de pequeno porte, caso o tratamento de dados não seja feito em larga escala. Além disso, a União Europeia recomenda a nomeação de encarregado para os agentes de pequeno porte nos casos em que: (i) se processe dados pessoais para direcionar publicidade, através de motores de busca com base no comportamento online dos indivíduos e (ii) se processe dados relacionados a genética e saúde para hospitais. Estas sugestões podem ser encontradas no seguinte link: https://ec.europa.eu/justice/smedataprotect/index_en.htm

Além disso, cumpre destacar que, assim como agentes empresariais de pequeno porte, outras pessoas físicas e entidades não empresariais, como ONGs, podem enfrentar dificuldades semelhantes. Portanto, seria importante uma flexibilização também em relação a estes entes.

Para a designação de Encarregado, a União Europeia criou exceções para empresas que não tem o tratamento de dados como parte de suas atividades essenciais, isto é, as atividades primárias das empresas (Recital 97, GDPR). Ainda, a designação de Encarregado pode ser dispensada para empresas que não realizam o tratamento de dados em larga escala, isto é, operação em grande escala com objetivo de tratar uma quantidade considerável de dados pessoais em nível regional, nacional ou supranacional que poderia afetar número grande de titulares de dados, e que poderiam acarretar possivelmente em alto risco (Recital 91, GDPR). Outros critérios para definir se um tratamento é realizado em larga escala, de acordo com o *Working Party* 29, é avaliar: (i) o número de titulares de dados sujeitos ao tratamento (número determinado ou proporção de uma população relevante); (ii) volume dos dados ou o leque de diversidade de dados sendo tratados; (iii) a duração ou permanência da atividade de tratamento; (iii) a extensão geográfica da atividade de tratamento[39].

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

Estabelece também o *Working Party* 29[40] que o tratamento de dados por pessoas físicas (como de um paciente por um médico ou de condenações e ofensas criminais por um advogado), logo, não abrangem tratamento de larga escala, de forma que a designação de DPO, neste caso, poderia ser dispensada. A mesma conclusão se aplica a diversas empresas de pequeno porte e microempresas, que possuem volume de dados, número de titulares, duração e extensão geográfica do tratamento reduzida.

Assim, entendemos que estes critérios poderiam ser aproveitados pela Autoridade para dispensar a exigências de nomeação de Encarregado para agentes de pequeno porte. Ainda, vale ressaltar que, muito embora a LGPD exija a indicação de DPO, a lei não deixa claro se o Encarregado poderá exercer a mesma função para outras empresas (isto é, se uma mesma controladora poderá compartilhar um Encarregado com outras controladoras). Tal possibilidade é prevista em normativa europeia, de forma que duas ou mais controladoras possam contratar um mesmo Encarregado, contanto que ele seja facilmente acessível e possa seguir com seu papel individualmente sem conflito de interesses entre as empresas. A terceirização de DPO, neste formato, pode importar em uma redução de custos comparada à contração de um DPO exclusivo para o agente. Assim, entendemos que a Autoridade poderia esclarecer essa possibilidade a partir de regulamentação futura, facilitando a gestão de recursos de agentes de pequeno porte na adequação à LGPD.

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

O relatório de impacto é um relevante instrumento de mitigação de riscos e eventuais problemas relacionados à violação dos direitos dos titulares, de forma que, ao reduzir riscos, há possivelmente uma diminuição de custos e futuras despesas, além de se possibilitar a detecção de falhas.

Por outro lado, a elaboração de um relatório de impacto também pode representar custos elevados para os agentes de menor porte. Desta forma, sugere-se que haja uma flexibilização quanto aos critérios e modelos de relatório, para que se tornem mais simples ou mais completos a depender da

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

especialidade do setor. Assim, atividades relacionadas a questões de saúde, por exemplo, podem demandar um relatório mais completo.

Portanto, seria importante que a ANPD determinasse modelos mais simples ou mais completos a serem adotados para setores específicos, à medida da necessidade dos riscos envolvidos.

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

Em decorrência da sensibilidade do tema, o tratamento destes dados pode resultar em custos mais elevados aos agentes de pequeno porte. Portanto, seria pertinente o fornecimento, pela ANPD, de orientações mais específicas sobre como se adequar aos regulamentos, transmitidas de forma coesa e didática.

Vale ressaltar, a flexibilização, para agentes de pequeno, do regulamento referente ao tratamento dos dados em questão é extremamente sensível, à medida em que exigem uma maior cautela e proteção.

Caso fosse feita a flexibilização, seria interessante que se utilizasse, assim como sugerido em outros pontos, o critério de setores de atividade, com modelos mais simplificados ou mais completos, a ser determinado pela ANPD. Ademais, seria pertinente que a autoridade orientasse de forma clara como garantir e autenticar o consentimento do tratamento e coleta destes dados.

Quanto aos dados de crianças e adolescentes, a cautela no seu tratamento se justifica pela vulnerabilidade da situação dos titulares em questão, presumido que estão menos cientes dos riscos do tratamento de seus dados para finalidades que possam não ser adequadas, e que, em vista de sua capacidade jurídica reduzida, não respondem por decisões tomadas quanto ao tratamento de seus dados (a exemplo, ao consentirem com o tratamento de seus dados).

Por fim, é relevante ressaltar a necessidade de um posicionamento mais contundente por parte da autoridade sobre as demais bases legais aplicáveis aos dados de crianças e adolescentes.

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

Um programa de governança de dados deve ser entendido como parte de uma lógica de governança mais ampla, que abrange boas práticas para a elaboração de políticas internas, planos de resposta a incidentes, mecanismos de supervisão internos e análise de riscos em geral. Trata-se de um arcabouço de práticas que não pertence à realidade empresarial da esmagadora maioria dos agentes econômicos de pequeno porte no Brasil. Exigir a implementação de uma política de governança de dados para pequenas empresas, portanto, significaria impor gastos desproporcionais para esses negócios.

Não se menosprezam aqui, evidentemente, as consequências positivas que tais programas poderiam ter para essas empresas, que no longo prazo acabariam mesmo por se valorizar, ao estabelecer uma maior relação de transparência e confiança com os titulares de dados e mitigar eventuais prejuízos futuros com a violação de direitos nessa seara. Contudo, dada a realidade dos pequenos negócios no Brasil e a delicada conjuntura econômica que ainda reflete os efeitos da pandemia, seria essencial que fossem flexibilizados os requisitos para a implementação de um programa de governança de dados para as pequenas empresas. Também seria importante que a ANPD atuasse de forma pedagógica quanto a essa exigência, fornecendo guias práticos para sua implementação, bem como *templates* de procedimentos, políticas, notificações e demais instrumentos que compõem tais programas, como fazem as autoridades europeias.

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

Primeiramente, é importante destacar que não existe no texto da LGPD uma definição mais ampla quanto a quais serão os requisitos que a ANPD implementará em matéria de segurança de dados pessoais. Justamente por isso, o assunto é objeto de uma outra Tomada de Subsídios, iniciada recentemente pela Autoridade[41]. Diante dessa ausência momentânea de regras em caráter geral, há naturais dificuldades de vislumbrar exatamente como

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

seriam os requisitos específicos exigidos dos agentes econômicos de pequeno porte.

Dito isso, a implementação de políticas de segurança relativa à proteção de dados pessoais eleva as práticas técnicas e organizacionais de empresas, exigindo um maior compromisso de funcionários na gestão de informações pessoais. Atualmente, a maioria dos agentes de pequeno porte não dispõem de medidas adequadas que garantam a segurança da informação de forma sofisticada. Empresas de menor porte ainda possuem reduzidas salvaguardas de segurança da informação, muito distantes das melhores práticas das grandes organizações, que investem vultosos recursos nesse tipo de proteção. Como é sabido, os custos de sistemas como esses são extremamente relevantes e, portanto, fora da realidade de boa parte das pequenas empresas.

Dessa forma, a política de segurança relativa à proteção de dados pessoais nos agentes de pequeno porte deve ser mais bem direcionada a suas peculiaridades, de forma a preencher a lacuna entre as disposições legais e sua compreensão e percepção de riscos à segurança da informação. Na prática, esta orientação deve vista como um guia de entrada que permita a esses agentes relacionar adequadamente suas atividades de tratamento com as disposições legais, de forma que possam identificar as medidas de segurança relevantes que devem implantar.

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

Como comentado na questão sobre o programa de governança, acima, a avaliação sistemática de riscos não faz parte da realidade empresarial da maior parte dos agentes econômicos de pequeno porte, posto que implica implementar uma vasta gama de práticas, que inclui o mapeamento de atividades de tratamento de dados, matrizes de riscos conforme atividades e planos de ação para adequação à LGPD. Cada uma dessas etapas exige dos agentes conhecimento das complexidades e peculiaridades da legislação, tais como as definições específicas da lei, sua abrangência e exceções à aplicação, bases legais e condições de transferência internacional de dados, entre outros requisitos específicos. Dessa forma, a condução de uma avaliação sistemática de riscos é demasiadamente custosa às empresas, seja quando essa atividade é terceirizada a partir de consultorias técnicas e jurídicas, seja pela conscientização de funcionários a partir de workshops, treinamentos e implementação de políticas internas.

A exigência de uma avaliação de riscos, portanto, deveria ser flexibilizada para as pequenas empresas no que for possível, talvez segregando os agentes de pequeno porte pelo volume e/ou tipo de dados com que lidam, e a partir disso estabelecendo obrigações mais condizentes com sua prática. Paralelamente a isso, e em linha com as experiências internacionais, entendemos que a autoridade nacional poderia envidar esforços para elaborar guias práticos, em linguagem facilitada para a implantação de processos que compõem a avaliação sistemática de riscos à privacidade, além de oferecer *templates* de documentos (matrizes de riscos, inventários de dados etc.) que possam ser preenchidos com mais facilidade pelos agentes de pequeno porte.

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

Inicialmente é importante que a Autoridade defina as exigências regulatórias de modo claro e objetivo, de modo que as pessoas físicas e empresas, especialmente de pequeno porte, possam entrar em conformidade sem entraves desnecessários. Conforme destacado anteriormente, o custo de entendimento das exigências regulatórias pode se mostrar demasiadamente custosa às empresas caso não sejam definidas regras claras.

Embora o direito de portabilidade de dados deve seguir diretrizes ainda não regulamentadas pela autoridade nacional (Art. 18, V, LGPD), a garantia desse direito implica no investimento de recursos tecnológicos específicos e treinamento de funcionários que podem significar custos elevados para agentes de pequeno porte. São custos financeiros relacionados à gestão e criação de processos que envolvem localização e identificação de dados dos titulares e sua padronização em um espaço de tempo adequado e razoável. Os agentes de pequeno porte teriam também de criar canais e processo aptos a atender de maneira eficaz e adequada os pedidos de portabilidade de dados pessoais, podendo impor dificuldades operacionais consideráveis.

Vale ressaltar, que, conforme o entendimento da autoridade inglesa de proteção de dados pessoais, uma “taxa razoável” pelos custos administrativos do cumprimento da solicitação poderia ser cobrada do titular solicitante, caso a solicitação seja manifestamente infundada ou excessiva. A implementação dessa taxa poderia ser amparada por regulamentação da ANPD para agentes de pequeno porte, o que facilitaria o atendimento ao direito de portabilidade por pequenas empresas.

Ainda, deve-se mencionar que, conforme mandamento do Art. 40 da LGPD, poderá a ANPD dispor sobre padrões de interoperabilidade para fins de portabilidade. Uma sugestão, portanto, seria oferecer padrões de interoperabilidade mínimos pelos quais empresas de pequeno porte poderiam se guiar.

Adicionalmente, soluções podem surgir dentro do próprio mercado para facilitar aos agentes de pequenos realização da portabilidade de dados pessoais. A exigência de portabilidade pode disseminar práticas de padronização e estruturas de compartilhamento de dados entre os próprios agentes, facilitando sua interação.

Apesar dos custos e desafios mencionados, é reconhecido que a portabilidade de dados é fundamental para aumentar a concorrência em setores que dependam da utilização de dados pessoais. A definição regras claras para o tratamento de dados e para a migração de dados significa aumento da competitividade nesses mercados, com impactos positivos sobre o bem-estar do consumidor, entre outros benefícios.

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

Entendemos que o uso de *sandboxes* regulatórios poderiam ser implementados pela Autoridade para promover a inovação em agentes de pequeno porte. Como antecipado, o uso de *sandboxes* regulatórios permite que, em espaços experimentais, empresas e seus modelos de negócios inovadores que não se encaixem totalmente no arcabouço regulatório vigente possam operar em caráter temporário. Isto pode ocorrer desde que atendidas algumas condicionantes que podem limitar aspectos como, por exemplo, o número de usuários, a prestação do serviço em uma área geográfica limitada ou o período no qual o produto pode ser oferecido no mercado.

O uso de *sandboxes* regulatórios já tem sido prática recorrente internacional nos setores financeiro e, mais recentemente, tem sido incorporado no setor regulado de telecomunicações. Sobre este último, vale ressaltar que a Agência Nacional de Telecomunicações (ANATEL), não só tem mantido recorrente troca de conhecimento com agências estrangeiras a respeito da implementação de *sandboxes* no setor regulado (como a agência colombiana de telecomunicações), como em 2020, a partir da Consulta Pública nº 65, recolheu subsídios de empresas do setor sobre a possibilidade de reforma regulatória que incluísse entre seus principais pontos, a inclusão de modelos de *sandboxes* regulatórios. Em matéria de privacidade e proteção

de dados, a autoridade nacional inglesa de proteção de dados, ICO, já implementou, em 2018, modelo de *sandbox* regulatório que permitia a empresas com modelos de negócios inovadores contassem com o apoio, a orientação e supervisão da autoridade.

Dessa forma, entendemos que a ANPD poderia valer-se da flexibilização de algumas normas para startups e agentes de pequeno porte para garantir o desenvolvimento de seus projetos inovadores, mesmo observando princípios e diretrizes de proteção de dados e segurança da informação. Inclusive, em se tratando de proteção de dados pessoais e privacidade, entendemos que a flexibilização de regras condicionada à operação de empresas em espaço, tempo e com número de usuários limitados e com a supervisão da Autoridade, reduziria os riscos de violações de dados e, em caso de um incidente de segurança, favoreceriam a adoção, de forma mais assertiva, de medidas técnicas para suprir eventuais danos causados42.

Vale ressaltar que os *sandboxes* também podem contribuir para a facilitação de financiamento de modelos de negócio inovadores, sendo mais um atrativo à sua implementação. De acordo com relatório da Autoridade de Condutas Financeiras do Reino Unido (FCA), 40% das empresas que participaram do *sandbox* inaugural para serviços financeiros em 2017 receberam investimento durante ou depois do período de experiência em regime de *sandbox43*. Ressalta-se, ainda, que a implementação de *sandbox* regulatórios contribui para estreitar a relação entre reguladores e empresas inovadoras, de forma que o conhecimento gerado a partir de inovações pode contribuir para criação de novas regulações e políticas públicas.

Além disso, também podem ser utilizados, conforme previsto na GDPR, mecanismos de aproximação entre associações e organizações e a autoridade de dados de modo a aproximar seu contato, troca de informações e desenvolvimento institucional. Podem ser previstos selos e certificações de obtenção facilitada e não tão onerosas destinados a agentes de pequeno porte que demonstrem inovação perante a proteção de dados pessoais, bem como esses mesmos mecanismos e código de condutas formulados por associações ou organizações para promover não somente inovação tecnológica, mas também jurídica e institucional. Tais códigos de conduta podem ajudar a diminuir custos com relação à adaptação de regras e permitir o direcionamento de esforços e recursos em outro sentido.