RIO DE JANEIRO, 2021

Consulta Pública ANPD:

Pequenas e médias empresas e startups

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

RESUMO EXECUTIVO

A promulgação da Lei Geral de Proteção de Dados - LGPD, Lei 13.709/2018 - marcou a entrada do Brasil no rol de mais de 100 países com legislação sobre o tema. Além de garantir a proteção dos direitos do cidadão, a lei representa mais um passo favorável à inserção do Brasil no comércio internacional, principalmente em mercados mais maduros no tratamento de informações pessoais por parte das empresas como a União Europeia.

O desafio principal no momento é a implementação da lei, sem afastar as particularidades inerentes a cada setor. Em um debate público sobre a adequação à Lei Geral de Proteção de Dados, a diretora da Autoridade Nacional de Proteção de Dados (ANPD) Miriam Wimmer destacou que o órgão está atento à necessidade de adequar o texto legal à realidade das micro e pequenas empresas brasileiras, sendo essa uma das prioridades a serem tratadas na regulamentação.

No âmbito das pequenas e médias empresas, a adequação ainda é vista como uma burocracia draconiana e potencialmente inviabilizadora para uma parcela dos pequenos negócios. Em que pese a entrada em vigor da lei, um levantamento realizado pela ICTS Protiviti revelou que até dezembro de 2020, cerca de 82% das empresas ainda estavam atrasadas com as ações de adequação. A falta de preparo atinge em particular pequenas e médias empresas e dentre os motivos mais citados estão a falta de conhecimento técnico na área de proteção de dados dos profissionais envolvidos e falta de capital para investir nos processos de adequação.

Diante deste panorama, em 29 de janeiro de 2021, a ANPD lançou uma Consulta Pública para coletar subsídios sobre a regulamentação da aplicação da Lei Geral de Proteção de Dados para microempresas e empresas de pequeno porte, e, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos.

A consulta contou com contribuições da sociedade civil e o tema que integra a agenda regulatória 2021/2022 da ANPD, divulgada no dia 28 de janeiro. Diante disso, as orientações da ANPD sobre as pequenas e médias empresas deverão ser conhecidas até julho/2021.

O ITS participou da Consulta Pública, endereçando desafios voltados para a adequação nesse setor - dificuldades orçamentárias, técnicas e de implementação -, apresentando as oportunidades e mapeando algumas experiências internacionais neste tema, tais como a da Austrália e a do Reino Unido.

Compreendemos que um olhar para mercados mais maduros na discussão sobre privacidade, como é o caso dos países da União Europeia, ajudará o Brasil a tecer parâmetros de regulamentação da Lei Geral de Proteção de Dados (LGPD).

Nos países europeus e na Austrália, por exemplo, as respectivas leis de proteção de dados foram ajustadas considerando as possibilidades das micro e pequenas empresas, como a inexigibilidade de contratação de um profissional especializado e a dispensa da obrigação de se manter um registro do tratamento de dados para os pequenos negócios. É partindo dessas análise que compartilhamos, a seguir, os comentários submetidos à Autoridade.

PRINCIPAIS RECOMENDAÇÕES

1. **Elaboração de "Privacy Checklist"** voltado para pequenas e médias empresas, com citação de etapas claras e objetivas para adequação.

2. **Criação de espaço online,** contendo orientações específicas para diferentes setores, como saúde por exemplo.

3. **Criação de órgãos internos especializados na ANPD** que possam avaliar os riscos e as melhores formas de mitigação, representando um meio de conferir maior clareza para a implementação de mecanismos de proteção de dados pessoais.

4. **Criação de "Innovation Hub",** em que se estabelece parceria com outros órgãos públicos para auxiliar nos processos de adequação dos negócios, sanar dúvidas e prestar suporte no que seja necessário para que a proteção de dados seja uma consideração constante no decorrer da empreitada. Essa perspectiva faz com que seja possível que essas empresas (usualmente startups) possam dar vazão às suas obrigações de "***privacy by design***".

5. **Sugestões de técnicas regulatórias (*regulatory sandboxes*).** Ferramentas que permitem que sejam postas em prática inovações dentro e ambientes regulados e sob a supervisão de uma autoridade estatal reguladora. Há um aprendizado mútuo. O projeto pode se desenvolver e ser testado e a autoridade consegue visualizar de maneira mais direta os riscos e potenciais consequências (e inclusive interferir se necessário) das inovações.

SUMÁRIO

1. QUAIS SÃO OS DESAFIOS/PROBLEMAS REGULATÓRIOS RELACIONADOS AO TEMA?

Dentre os desafios e problemas relacionados à implementação da proteção de dados por agentes de menor porte podemos destacar pelos menos três elementos: **(i)** o caráter principiológico da Lei Geral de Proteção de Dados Pessoais ("LGPD") que faz com que seja necessária uma atuação da autoridade para prestar mais concretude sobre como implementar a norma; **(ii)** a disponibilidade de recursos econômicos e administrativos para fazer o processo de implementação à LGPD; e **(iii)** conscientização quanto os ganhos e oportunidades de adaptação à lei.

A combinação desses três elementos leva a pelo menos três desafios que serão analisados abaixo:

(1) Familiarizar-se e compreender as exigências da Lei Geral de Proteção de Dados

Em um cenário em que ainda se está desenvolvendo uma cultura de proteção de dados, as organizações menores ainda precisam se familiarizar com as exigências da lei de proteção de dados.

A LGPD traz a necessidade de as organizações adequarem suas práticas internas. Para tanto, é importante ter conhecimento e clareza sobre como poder dar cumprimento aos requisitos trazidos pela lei. A normativa, contudo, não sempre traz de maneira sistemática os diferentes passos que devem ser seguidos. Adicionalmente, mesmo expressões chave como "termo de uso", "política de privacidade" ou "fluxo de dados" não estão presentes na lei. Dessa forma, existem potenciais barreiras à compreensão do que necessita ser efetivamente adequado, em que devem consistir as modificações nas práticas de governança de dados, e que documentos específicos devem ser produzidos.

(2) Orçamento e recursos humanos suficientes para implementar a LGPD

A proteção de dados surgiu em função da necessidade de se proteger o indivíduo quanto ao risco de mau uso de seus dados. É razoável que a lei seja flexível para dar conta do grau de risco referente à natureza de dados tratados, ao tratamento em si e ao contexto em que eles são tratados.

Diante disso, considerando o princípio da proporcionalidade, é compreensível que haja uma diferença entre a empresa detentora de milhões de dados pessoais e uma empresa que mantém quantidade de dados reduzida. Do contrário se pode onerar demais a empresa menor, o que pode inviabilizar diferentes negócios - considerando os investimentos de adaptação e riscos de sanções.

Em países com cultura de proteção de dados já mais maduras, como a Austrália e os 27 países da União Europeia, cuja legislação regional, o GDPR,

serviu de base para a brasileira, a lei foi ajustada às possibilidades das micro e pequenas empresas, como explicitamos no setor de experiências internacionais de resposta a esta consulta.

(3) Realização de mapeamento de dados e análise de gaps e monitoramento contínuo de compliance

Neste tópico é importante considerar que não há, na LGPD, diferenciação de tratamento e obrigações entre as grandes empresas e as médias e pequenas empresas quanto às adequações ao regramento de proteção de dados. Este apontamento é importante porque o enquadramento à LGPD é potencialmente custoso - por envolver necessidade de serviços conjuntos de segurança, tecnologia, jurídico e compliance - o que significará mais uma dificuldade significativa sobretudo aos pequenos negócios.

Temos no Brasil uma realidade na qual diversas empresas não possuem proteções jurídicas mínimas, como contratos personalizados e bem formulados com fornecedores e prestadores de serviço, enquadramentos às regras consumeristas, regimentos internos que refletem uma cultura empresarial desejada, enquadramentos fiscais corretos ou, ainda, sem elementos básicos de governança e compliance. Nesse cenário, fica o questionamento de como serão tratadas as determinações da LGPD para empresas que já possuem dificuldades de cumprir com requisitos de outras leis como proteção do consumidor, ou mesmo leis setoriais.

Atividades mais complexas como mapeamento de dados, análises de gaps ou lacunas organizacionais ou mecanismos contínuos de compliance dependem de um esforço maior da organização. É um desafio poder dar vazão a essas obrigações.

2. EXISTEM SUGESTÕES PARA ENDEREÇAMENTO DO PROBLEMA?

(1) Conscientização e ferramentas simplificadas:

O primeiro passo deve ser a conscientização das organizações da importância da lei e apoio a sua adequação.

A autoridade pode buscar a organização, participação ou apoio a eventos e atividades que incentivem o conhecimento e promoção da lei e de seus benefícios para organizações de menor porte.

Deve-se apresentar ferramentas simples que não somente expliquem a adequação, mas sim que auxiliem diretamente no processo. Como se percebe abaixo, diversas autoridades de proteção de dados de diferentes países proporcionam ferramentas com as quais as organizações podem: **(i)** entender se a lei se aplica a elas e em que medida; **(ii)** realizar uma auto-avaliação para verificar o quanto já estão compatíveis e o que precisa ser adequado; **(iii)** modelos de docu-

mentos, com instruções práticas de como usá-los, para que servem e em que se adapta; e **(iv)** padronização de procedimentos.

(2) Mecanismos dedicados de auxílio e apoio:

Adicionalmente, é prática de muitas das autoridades de proteção de dados administrar mecanismos específicos para auxílio e suporte de organizações de menor porte. Os desafios de adaptação são grandes e mesmo como ferramentas e modelos surgem dúvidas que são pontuais e muitas se relacionam a cada organização.

Os altos custos relacionados à contratação de especialistas para dar auxiliar no processo de adequação muitas vezes são proibitivos para organizações menores. Um corpo dedicado de apoio organizado pela autoridade pode em muito facilitar o processo.

Autoridades como a inglesa, por exemplo, trocam o apoio pela possibilidade de publicação do processo de adequação como "estudos de caso" em que outras organizações podem se espelhar.

Adicionalmente, por ser um grupo dedicado, podem mais facilmente encontrar soluções comuns gerando uma espécie de padronização ou "jurisprudência" sobre como atuar frente problemas e práticas recorrentes.

(3) Uso proporcional de mecanismos de sanção e fiscalização:

Mecanismos de fiscalização e sanção tendem a ser custosos tanto para a administração pública, quanto para as organizações afetadas. A complexidade dos procedimentos também leva a aconselhar um tratamento mais amigável.

A fiscalização e a sanção são instrumentos importantes de política pública e têm o seu papel. Contudo, para organizações menores a abordagem educacional somada a um apoio de adequação pode ter um impacto mais amplo. Em estudo no Canadá (explicitado abaixo), uma das mudanças mais significativas sugeridas é que o uso de sanções seja proporcional para não impedir o funcionamento de serviços e negócios que estejam buscando cumprir com a regulação.

3. QUAIS SÃO AS OPORTUNIDADES RELACIONADAS AO TEMA?

(1) Transformação digital:

Com a busca por conhecimento sobre organização e segurança de informações e a cultura colaborativa, em que diferentes áreas trabalham em cooperação para o tratamento ético e seguro de dados, maior confiabilidade nas relações comerciais e mais transparência com o titular de dados.

(2) Participação no mercado internacional:

trata-se de grande oportunidade para tratativas com clientes e transações

comerciais internacionais, já que países que têm leis de proteção de dados limitam operações com países sem legislação correspondente.

4. QUAIS SÃO AS EXPERIÊNCIAS INTERNACIONAIS SOBRE O TEMA?

(1) União Europeia:

Mais abaixo se explora em detalhes como a UE trata do tema, mas importante ter em mente que na região a regulação aprovada (GDPR) é pensada para servir de elemento de harmonização e facilitar que as diferentes empresas (particularmente as de menor porte) possam atuar no mercado econômico comum.

O Considerando 13 do GDPR já deixa claro que o tratamento a ser dado a micro, pequenas e médias empresas deverá ser diferenciado, definindo-se o seguinte:

"Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controlo, são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento."

A lógica a ser utilizada parece ser que essas empresas de menor porte devem poder ficar isentas ou ter procedimentos mais simplificados quanto a certos elementos da lei.

Um ponto a ser tomado em consideração é que, ainda que se tome como ponto de partida a noção de MPES (empresas com menos de 250 trabalhadores e um valor de faturamento anual de até 50 milhões de euros), esta não é a única consideração. Ou melhor, a consideração mais relevante se dá quanto à natureza do tratamento de dados, envolvendo consideração quanto ao volume e tipo de dados e a característica do processamento.

(2) Reino Unido

Após o Brexit, o Reino Unido aprovou a própria legislação de proteção de dados (UK-GDRP). Devido à semelhança com o modelo anterior, a maioria das leis de proteção de dados para pequenas empresas continuaram as mesmas, salvo para as que tiverem contatos ou consumidores na Zona Econômica Européia - nesse caso, as normas da UE podem ser aplicadas. Para auxiliar as empresas na adequação, a ICO (autoridade de proteção de dados inglesa) tomou as precauções para garantir que pequenas empresas compreendessem se seriam ou não afetadas. Apresenta um "quiz" com perguntas simples e, ao final, sugere ações e um diagnóstico do que deve ser feito para a adequação.

Dessa forma, a preocupação com pequenas empresas continua seguindo

a lógica do GDPR europeu. É incentivada uma visão positiva sobre as normas de proteção de dados com destaque aos benefícios advindos do compliance. Por exemplo, mesmo com um volume de dados menor, caso a empresa siga os procedimentos necessários para proteger informações e lidar com solicitações, aumentará a confiança no seu negócio e economizará tempo.

A ICO possui um sistema muito eficiente online que fornece uma espécie de consultoria gratuita aos pequenos negócios. Primeiro, recomenda empresas a realizarem um pequeno auto-avaliação para verificar se a Lei de Proteção de Dados é aplicável ao seu negócio. Após, por meio de perguntas objetivas e de fácil compreensão, a ferramenta faz o diagnóstico do negócio em relação ao Data Protection Act ou GDPR, se está regular ou não e o que precisa ser feito para a adequação. Caso ainda restem mais dúvidas, a ICO fornece um contato específico para serviço de aconselhamento para pequenas organizações.

O Reino Unido também conta com algumas instituições voltadas ao auxílio de pequenas empresas. O ICO Innovation Hub foi criado para colaborar com reguladores, oferecendo experiência em proteção de dados para um gama maior de empresas inovadoras. O Legal Access Challenge foi uma das inovações auxiliados pelo Hub, o projeto permitiu que indivíduos, famílias e pequenas empresas tivessem o apoio jurídico que necessitavam, incluindo um chatbot e outras plataformas. Além disso, a FSB, the “Federation of Small Business”, oferece assistência legal a seus membros através do “FSB Legal Hub”.

(3) Austrália

O Privacy Act, lei australiana de privacidade de dados, não se aplica à maioria das pequenas empresas. Na Austrália, uma pequena empresa é aquela com um faturamento anual de até US $3 milhões.

O Australian Information Commissioner Office fornece uma “privacy checklist” para pequenas empresas com perguntas diretas e simples verificarem a necessidade de adequação aos “Australian Privacy Principles”(APPs). São treze princípios que buscam oferecer flexibilidade a uma organização ou agência para adaptar suas práticas de tratamento de informações pessoais aos seus modelos de negócios e às diversas necessidades dos indivíduos.

Para além da checklist, há um espaço online que detalha quais pequenas empresas estão sujeitas ao Privacy Act em seu site, por exemplo, pequenos provedores de saúde ou pequenas empresas associadas a negócios sujeitos ao Privacy Act.

(4) Canadá

PIPEDA (Personal Information Protection and Electronic Documents Act) é a lei canadense de privacidade de dados que se aplica à coleta, uso ou divulgação de informações pessoais no curso de uma atividade comercial. A PIPEDA não faz menção a pequenos e médios negócios, havendo o entendimento de que devem se adequar respeitando os princípios estabelecidos na lei. A lei vem sendo

criticada por não ser acessível a estas empresas e já foram feitas propostas de mudanças para modular a lei para albergar MPEs (inclusive na recente "Policy Proposal for PIPEDA Reform to Address Artificial Intelligence").

No site do Office of the Privacy Commissioner of Canada existe o auxílio devido para que negócios se adequem à legislação de proteção de dados No site do Office of the Privacy Commissioner of Canada existe o auxílio devido para que negócios se adequem à legislação de proteção de dados com guias e mecanismos para tirar dúvidas. Um ponto a ser notado é que no Canadá pequenas empresas são aquelas que possuem entre 1 e 99 empregados e médias empresas as que possuem entre 100 e 499 empregados.

5. QUAIS SÃO OS CRITÉRIOS QUE DEVERIAM SER CONSIDERADOS NA DEFINIÇÃO DE AGENTES DE TRATAMENTO DE DADOS DE PEQUENO PORTE?

(1) Considerações advindas diretamente da legislação:

No contexto brasileiro, um dos elementos que aparece na legislação que serve de indicativo de como se deve diferenciar agentes de pequeno porte de outros quanto ao tratamento de dados pessoais se encontra na **exceção da exigência de nomeação do Encarregado**. Esta é ventilada no art. 41, § 3º da LGPD - sujeito a regras específicas da ANPD -, em função do **porte da entidade** ou do **volume de operações** de tratamento de dados.

É importante ressaltar que essa diferenciação leva em consideração dois elementos relevantes como critérios para a definição de agentes de tratamento de pequeno porte: **1 - critérios sólidos para análise de risco da atividade; 2 - a definição acolhida para pequenas e médias empresas** para fins de aplicação da LGPD (deve-se definir se a definição será com base no número de funcionários ou da receita bruta da empresa, a exemplo das definições constantes na Lei Complementar 123/2006).

(2) Considerações sobre características da empresa:

No Brasil temos a figura do microempreendedor individual, definido este como pessoa que trabalha por conta própria e se legaliza como pequeno empresário optante pelo Simples Nacional (Lei Complementar 128/2008). Considerando o fato de que o microempresário pode possuir um único empregado, é preciso considerar, neste contexto, os papéis dos agentes de tratamento de dados e do encarregado, cujas atividades podem ser concentradas, na prática, na mesma pessoa natural.

Diante do exposto, à princípio, o critério da natureza da atividade e dos dados coletados deve prevalecer sobre o tamanho da organização quando da análise da exceção para nomeação do encarregado, uma vez que o risco para o titular, muitas vezes, é o mesmo, independentemente do tamanho da empresa.

No mesmo sentido determina o relatório do Comitê Europeu para Proteção de Dados - EDPB (p. 35): *"the risk-based approach promoted by the legislator in the text should be maintained, as risks for data subjects do not depend on the size of the controllers."*

E, no mesmo sentido, exemplifica Bruno Bioni: "não faz sentido uma rede de padarias, ainda que com muitos funcionários mas sem nenhum tipo de tratamento de alto risco de dados dos clientes, ter um DPO. Já uma startup na área da saúde, ainda que com poucos funcionários, mas com uma atividade de tratamento de dados de alto risco, deveria ter um DPO sim". Contudo, como explicitado anteriormente, é necessário delimitar de forma mais precisa os critérios para análise do risco da atividade empregada.

(3) Considerações sobre análise de riscos:

Os critérios para escalonamento e classificação dos riscos devem levar em consideração o processamento em grande escala e categorização dos dados.

O processamento em grande escala pode ser interpretado a partir de operações de processamento de dados que requerem monitoramento de indivíduos em larga escala, volume de dados, duração do processamento ou distribuição geográfica. A continuidade e regularidade do monitoramento também deve ser considerada, incluindo, nesta análise, a criação de perfil e marketing direcionado.

Quanto à categorização dos dados é possível considerar que processamento de dados sensíveis compreendem atividades de alto risco. No entanto, também é preciso fixar critérios para situações de tratamento de dados não sensíveis, mas que ensejam potenciais discriminações.

6. COMO A UNIÃO EUROPEIA TEM ATUADO PARA QUE AGENTES DE TRATAMENTO DE DADOS DE PEQUENO PORTE ESTEJAM EM CONFORMIDADE COM A GENERAL DATA PROTECTION REGULATION (GDPR)?

(1) Atuação conjunta:

Parte das dificuldades mais comuns se relacionam com a compreensão de como adaptar de uma maneira rápida, acessível e econômica (mantendo um alto nível de proteção) as obrigações procedimentais previstas na legislação aos processos do dia-a-dia de empresas de menor porte. A diminuição do ônus administrativo parece ser um dos grandes pontos levantados.

A estratégia comum da UE (através do "EDPB") aparentemente tem sido em duas linhas: (i) reforçar a compreensão dos diferentes agentes de noções elementares da proteção de dados; e (ii) desenvolver ferramentas que possam ser utilizadas mesmo por leigos para poder realizar avaliações de risco internas, e encontrar meios fáceis, padronizados de desenvolver proteções e salvaguardas.

Nesse sentido, atividades desenvolvidas dentro dessas estratégias incluem eventos com diferentes stakeholders, consultas e pesquisas para levantamento de dados, e desenvolvimento de ferramentas e guias que facilitem o compliance.

De um ponto de vista da ANPD, essas estratégias podem servir de norte para buscar uma atuação mais harmonizada e comum levando em consideração o tamanho e a extensão do país.

(2) Atuação de diversas Autoridades nacionais e locais de proteção de dados:

As autoridades nacionais e locais desenvolveram atividades diferentes, mas em comum destacamos as seguintes:

a. realizar **pesquisas** com agentes de tratamento afetados (de menor porte) para entender na prática as suas dificuldades. Um exemplo interessante de pesquisas, foram as realizadas pelas autoridades de proteção de dados da Bélgica (resultados aqui) e da Bulgária (aqui e aqui);
b. participar e organizar **atividades de conscientização** em que o grupo de stakeholders estejam presentes. De certa forma o principal ponto nos primeiros anos de vigência, como mencionado pelo Presidente do Conselho da ANPD, deve ser a educação e a geração de uma cultura de proteção de dados. Nestas se incluem também elementos de comunicação com o vídeo da autoridade francesa com um YouTuber;
c. disponibilizar **ferramentas simplificadas** desde guias, até documentos, "checklists" e formulários de auto-avaliação. Importante que tanto a informação seja acessível compatível com um nível muito básico de compreensão da legislação (desenvolvido para leigos), quanto seja prática e útil de uso imediato. O exemplo do mecanismos de auto-avaliação da autoridade do Reino Unido é indicativo, assim como o checklist; e,
d. ter uma **linha direta de aconselhamento** em que pessoal está dedicado a responder as principais dúvidas e aconselhar sobre como melhor proceder com relação à proteção de dados (desde adaptação até incidentes de segurança). Veja a ferramenta "Facilita RGPD" da Espanha e "helpdesk" do Reino Unido; outras que também possuem mecanismos similares como a autoridade da França, da Islândia, da Polônia, entre outras;
e. estabelecer uma **equipe dedicada que possa dar suporte à adequação** dos agentes de menor porte. Serve de "hubs" nos quais se compilam práticas, manuais e diretrizes. É um ponto focal acessível que mantém um histórico. Também serve como portal de acesso. Ilustrativo é seção de micro e pequenas empresas da autoridade do Reino Unido.

7. QUAIS SÃO OS IMPACTOS PARA AGENTES DE PEQUENO PORTE DA MANUTENÇÃO DO REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS?

Os principais impactos que existem da obrigação de manutenção de registro advêm do **ônus administrativo e da falta de pessoal especializado.** De um modo geral, agentes de menor porte estão focados em sua atividade central. Uma padaria de bairro pode ter a necessidade de tratar dados pessoais, mas a sua atenção se volta na venda de produtos aos seus clientes. Os dados pessoais existem muito provavelmente para meramente satisfazer as necessidades legais, seja de relações de trabalho, tributárias ou contratuais.

Operações envolvendo dados pessoais não somente devem ser em menor número como envolver menor risco. Obrigações complexas de registro de operações podem inviabilizar transações. O famoso caderninho de compras - possui diversos dados pessoais relacionados ao histórico de compras e de vendas. Em muitos lugares ainda é um meio importante e se baseia em uma relação de confiança. Exigir registro dos tratamentos pode tornar muito oneroso o processo ou obrigar a que esses negócios convivam com uma espécie de desconformidade.

Valeria **estabelecer ferramentas que incluam padrões mínimos de de registro e que sejam extremamente simplificados, compatíveis com os níveis de risco das atividades.**

8. QUAIS SÃO OS IMPACTOS DA NOMEAÇÃO DE UM ENCARREGADO DE DADOS AOS AGENTES DE PEQUENO PORTE?

Há que se entender que no contexto de agentes de pequeno porte incluem-se organizações de diferentes formatos, áreas e objetivos. A nomeação de um encarregado por impactar a elas de diferentes maneiras.

Seguindo a lógica de que o encarregado deve primeiramente servir de canal de comunicação, há que se ter em mente que em nem todas as situações há inclusive uma demanda suficiente para existirem ganhos na nomeação de um encarregado. Nesse sentido, propõe-se três níveis de recomendação quanto ao impacto de uma nomeação.

(1) Quando NÃO é recomendável a nomeação:

Atividades que não envolvem de maneira significativa dados pessoais, como no exemplo explorado acima da padaria de bairro, não têm muito a ganhar com a nomeação de um encarregado. Isso ocorre pela diminuta demanda ou pela inexistência de um risco significativo para os dados pessoais.

A nomeação serviria provavelmente para aumentar custos, burocracia, e muito provavelmente serviria a uma função meramente pró-forma. Poderia inclu-

sive passar um falso senso de confiabilidade que não estaria de acordo com a realidade.

(2) Quando é recomendável a nomeação:

Em algumas situações, ainda que provavelmente não fosse necessária a nomeação, potencialmente poderia ser positiva. Em alguns casos como por exemplo com a lida de dados sensíveis como em uma pequena clínica hospitalar, uma entidade de classe ou associação, ou mesmo áreas de maior obrigação regulatória em que se trata de um volume mais amplo de dados pessoais (um escritório de contabilidade para ilustrar).

Nesse sentido, ainda que haja um aumento do custo, da burocracia, pode servir a um propósito acautelatório de mitigação de riscos. Um vazamento de dados poderia vir a ter um custo direto (danos) ou indiretos (reputacionais) grandes.

Uma organização poderia, então, ter mais a ganhar com a nomeação de um encarregado. Seria igualmente no seu interesse ter alguém especialista que além de servir de canal de comunicação, também auxiliasse com críticas construtivas no processo de adaptação dos procedimentos internos.

(3) Quando deve ser obrigatória a nomeação:

Há atividades que efetivamente têm como um ponto nevrálgico o tratamento de dados pessoais. Nessas circunstâncias, independente do porte em si do agente, deve ser obrigatória a nomeação.

O famoso caso da empresa Cambridge Analítica parece ser ilustrativo. Era uma empresa com menos de 250 funcionários e faturamento que não atinge os 50 milhões de euros, no entanto, o seu serviço primordial dava-se pela análise de dados pessoais.

Outros exemplos podem existir em empresas Fintech. Muitas têm como elemento central a melhoria da análise de perfis de pessoas para determinar um escore de crédito.

Nesse sentido, por envolveram tantos dados pessoais e por o tratamento destes ser ponto central, há uma necessidade de maior cuidado. Para tanto, ainda que exista um impacto no negócio, o risco é tamanho que faz sentido que haja uma pessoa claramente responsável pela proteção de dados e que possa revisar as práticas internas e fazer constantes sugestões. Um encarregado serve a uma função tanto interna de prevenção, assim como social de satisfação de interesse dos titulares e da autoridade.

9. QUAIS SÃO OS IMPACTOS DA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS AOS AGENTES DE PEQUENO PORTE?

Relatórios de impacto à proteção de dados são documentos extremamente importantes para a proteção de dados pessoais em atividades de maior risco.

A LGPD, no entanto, não define claramente em que circunstâncias pode ser necessária a elaboração desse tipo de relatório. A indicação da lei é de que "quando o tratamento tiver como fundamento seu *interesse legítimo*" pode ser solicitado ao controlador. Esse indicativo parece pressupor um espaço de modulação dessa obrigação.

Não são todos os casos de tratamento com base em interesse legítimo que atingem um grau de risco suficiente para que seja necessário ou mesmo útil a realização de relatórios de impacto. No caso de agentes de menor porte, a tendência é que este seja ainda menor, pois os volumes de dados usualmente são mais baixos.

Devido aos altos custos destes relatórios certos tratamentos de dados (baseados em interesses legítimos) podem se tornar inacessíveis para MPEs. O custo de realização do relatório não aumenta necessariamente na mesma medida que o tamanho da empresa, sendo assim, representa proporcionalmente um aporte maior na composição de custos de um agente de menor porte que um de maior.

De um ponto de vista de equidade na concorrência, agentes maiores teriam vantagens de poder usar estes tratamentos e menores não. Até porque menores teriam maior dificuldade de compor esses custos dentro de seus cálculos financeiros.

Nesse sentido, é importante ter dois elemento em mente: (i) uma **simplificação metodológica** no tipo de relatório pode simplificar e possibilitar o uso mais extenso dessa ferramenta; e (ii) a **clareza quanto ao momento e as circunstâncias (critérios) em que os agentes são obrigados** a realizar essa análise pode tornar mais acessível e padronizar no mercado o uso da ferramenta.

10. QUAIS SÃO OS IMPACTOS DA IMPLEMENTAÇÃO DO TRATAMENTO DE DADOS, INCLUSIVE SENSÍVEIS E DE CRIANÇAS E DE ADOLESCENTES, EM CONFORMIDADE COM A LGPD AOS AGENTES DE PEQUENO PORTE?

Os agentes de tratamento que lidam com dados de crianças e adolescentes por excelência são escolas e creches. Nesse sentido, as instituições de ensino coletam e armazenam inúmeros dados pessoais (físicos e digitais), desde crianças e adolescentes até alunos maiores de idade, pais e colaboradores. Ademais, em um cenário de digitalização crescente da educação, acelerado pela pandemia, uma série de novos dados, como imagens de webcams e endereços IP, passaram a ser coletados e usados.

Todas as instituições terão de se adaptar (vale mencionar a publicação do CIEB e da UNESCO que reúne orientações práticas para gestores e gestoras educacionais), mas para pequenas instituições, como as creches de bairro, o desafio será maior. Muitas dessas pequenas instituições sequer possuem políticas de privacidade e ainda terão de fazer o levantamento de informações coletadas e sua finalidade. Ressalte-se que como a LGPD se aplica aos dados já coletados, tanto físicos quanto digitais, será necessário a análise das informações arquivadas como históricos escolares, avaliações de desempenho, contratos, dados bancários, etc., para verificar aqueles que poderão continuar armazenados e os que deverão ser eliminados.

Há aqui uma necessidade de transparência que se cristaliza na publicização de certas informações seja por meio de uma política de privacidade, em uma cláusula contratual, nos formulários de matrícula ou em qualquer aviso na plataforma educacional ou site.

Além disso, uma reestruturação da instituição deverá ser realizada, definindo a figura do encarregado mas também restringir o acesso de funcionários aos dados, desde a lista de presença, ou dados mais sensíveis, como etnia, religião e renda familiar, visando evitar possíveis vazamentos.

Destaca-se que o **tratamento de dados deve ser feito no melhor interesse da criança,** obrigação que leva à necessidade de ter um cuidado mais elevado.

Nesse contexto, as obrigações de proteção de dados de crianças devem trazer novos elementos tensão entre direitos que os agentes de pequeno porte provavelmente terão maiores dificuldades de resolver.

O exemplo relacionado às fotos de crianças realizados pelos pais em ambientes escolares ilustram esses desafios. Antes da entrada em vigor da lei era bastante comum que em funções escolares imagens que envolviam as crianças circulassem. Com a entrada em vigor, há uma tensão entre a responsabilidade da escola para definir políticas sobre o que ocorre no seu ambiente e os direitos das crianças e seus pais de ter memórias e compartilhá-las com seus conhecidos.

Casos na Irlanda e no Reino Unido explicitaram como as escolhas são difíceis. Há escolas que terminantemente proibiram a retirada de fotos em seus espaços para evitar qualquer responsabilização por potenciais violações de proteção de dados. Isso muito provavelmente é uma ação não necessária e até potencialmente exagerada frente a legislação vigente.

De outra forma, já se percebe que mesmo em escolas menores já se está buscando a utilização de novos meios tecnológicos potencialmente invasivos como chamadas pela via de reconhecimento facial. O desconhecimento dos riscos da tecnologia podem estar por trás desses usos.

Nesse sentido, em se tratando da proteção de dados de crianças e adolescentes **há um cuidado maior que deve existir e o impacto deve ser significativo nos diferentes processos de tratamento de dados. No entanto, pode existir um mérito na sua implementação mesmo em situações de menor porte.**

11. QUAIS SÃO OS IMPACTOS DA IMPLEMENTAÇÃO DO PROGRAMA DE GOVERNANÇA DE DADOS AOS AGENTES DE PEQUENO PORTE?

Programas de governança de dados são significativos para a proteção de dados pessoais, particularmente quando há um nível de complexidade maior de tratamento. Em situações de menor risco, programas de governança feitos sob medida parecem ser extremamente onerosos sem necessariamente gerar grandes mudanças organizacionais.

Imagine-se uma empresa com três funcionários, um programa de governança de dados pode ter impacto de custos altos sem necessariamente modificar de maneira significativa as práticas e rotinas das pessoas envolvidas.

A existência de **planos e ferramentas de governança modeladas para organizações de menor porte,** com sugestões fáceis de serem implementadas podem atingir o objetivo sem necessariamente sobrecarregar burocrática e financeiramente as organizações.

12. QUAIS SÃO OS IMPACTOS DA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA RELATIVA À PROTEÇÃO DE DADOS PESSOAIS AOS AGENTES DE PEQUENO PORTE?

Políticas de segurança são cada vez mais uma prioridade, haja vista os inúmeros incidentes que se apresentam. Estudos recentes indicam que o Brasil é particularmente vulnerável, sendo que mesmo em relação a pequenas e médias empresas há um alto percentual delas (63%) que já sofreram em alguma medida com algum incidente de segurança (particularmente vazamento de dados).

Nesse cenário, há que se entender a necessidade clara de desenvolvimento e implantação de medidas técnicas e administrativas de segurança nos diferentes níveis dos agentes.

A LGPD no art. 46 § 1º já deixa claro que há diferentes graus em que devem ser obrigatórias a utilização de medidas de segurança técnicas e administrativas. A título de critério, a lei estipula que serão “considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis”.

No caso de agentes de menor porte esses critérios devem ser somados ao da capacidade de absorver os diferentes custos. Isso não quer dizer não tomar as medidas de segurança necessárias, mas sim que deve existir espaço para a facilitação do modo como estes agentes devem implementar essas medidas.

De um lado, seria importante que a autoridade **incentivasse a criação de ferramentas acessíveis** e desenhadas para tratamentos de menor porte. Assim como a **promoção de mecanismos de conscientização** em conjunto com **formas de capacitação.**

Quanto a esse último ponto, leva-se em consideração que significativo percentual dos incidentes advém de erros humanos. Capacitação é crucial. Adicionalmente, há claramente uma lacuna na formação de profissionais nessa área em todo o mundo e no Brasil esta brecha é ainda mais significativa.

Agentes menores de dados, então, são obrigados a competir por profissionais em um cenário muito desfavorável. É importante que haja uma maleabilidade no sentido de dar conta dessas circunstâncias.

Facilidades nos instrumentos e clareza nas obrigações certamente reduzem custos e permitem que os diferentes agentes (inclusive os que não conseguem contratar profissionais especializados) possam também dar segurança aos dados pessoais que tratam.

13. QUAIS SÃO OS IMPACTOS DA IMPLANTAÇÃO DA PORTABILIDADE DE DADOS PESSOAIS AOS AGENTES DE PEQUENO PORTE?

O direito à portabilidade pode ter um impacto extremamente positivo para as PMEs. Esse direito diminui as barreiras de entrada e o efeito "lock-in" em que as pessoas tendem a se manter com um serviço que não necessariamente é o mais vantajoso para elas pelo fato de que é um esforço muito grande a troca de prestador de serviço. Ao possibilitar que o titular porte seus dados, permite que este inicie uma nova relação com um novo prestador já com todo o seu histórico anterior.

Nesse sentido, empresas de menor porte podem ter acesso a novos mercados consumidores. Elas têm a chance de oferecer seus produtos e prestar seus serviços para um quadro maior da população.

Igualmente, o direito à portabilidade de dados é um elemento essencial para garantir a livre escolha e proteção do consumidor em um ambiente digital competitivo. Como os indivíduos confiam em plataformas diferentes para realizar atividades essenciais, o conhecimento sobre proteção de dados e a implantação da portabilidade precisam ser cuidadosamente abordadas por todas as partes interessadas.

Apesar disso, existem dificuldades para a implementação desse direito. Os desafios englobam aspectos legais - como, por exemplo, a definição de quais dados são portáteis e parâmetros de atribuição de responsabilização em caso de incidente de segurança durante a transferência dos dados -, até técnicos - por exemplo, como permitir que indivíduos movam, copiem ou transfiram facilmente dados pessoais em diferentes plataformas de maneira segura e protegida.

As dificuldades e oportunidades desse direito devem ser analisadas em sentido geral, uma vez que não afetam apenas o âmbito de pequenas e médias empresas.

Em diversas circunstâncias, o exercício desse direito pode ser feito ainda

que por agentes de menor porte. Um consultório médico, por exemplo, pode entregar os dados dos pacientes (exames, prontuários, entre outros). Não há um impacto tão profundo na sistemática do serviço prestado.

No entanto, em diversos casos, a obrigação de portabilidade, de existir um meio que torne possível reutilizar os dados (efetivamente portar para outro local para realização do mesmo serviço) pode envolver um enorme custo. Hoje não existe uma obrigação e interoperabilidade de sistemas, então, existem inúmeros formatos em que dados são guardados e armazenados. **Uma obrigação muito ampla de portabilidade de dados para agentes de menor porte pode querer dizer ou a inviabilização de negócios, ou a monopolização (oligopolização) da utilização de sistemas que estes possam tornar os dados "portáveis" para satisfazer as obrigações deste direito.**

Com intuito de apresentar as problemáticas de implementação do direito,o ITS criou o repositório virtual: https://www.portabilidadededados.com.br/

O portal reúne as principais publicações nacionais e internacionais sobre o tema da portabilidade de dados e relatórios especializados, focando em quatro categorias principais: concorrência, proteção de dados, tecnologia e indústria.

14. QUAL INSTRUMENTO REGULATÓRIO PODERIA SER UTILIZADO PARA PROMOVER E INCENTIVAR A INOVAÇÃO NOS AGENTES DE PEQUENO PORTE?

A promoção da inovação é central tanto para o desenvolvimento social como econômico. Há que se buscar que a inovação seja responsável e saudável para a população tendo em vista demandas éticas e de direitos fundamentais. Diversas das transformações das últimas décadas relacionam-se direta ou indiretamente ao uso de dados. Dessa forma, há que se ter como um dos eixos da proteção de dados também a garantia de um ambiente que incentive a inovação e experimentação responsável.

Propõem-se que **não haja somente um foco em um instrumento regulatório,** mas sim que o incentivo à inovação responsável seja uma **preocupação transversal da ANPD.**

I) Aspectos relevantes da inovação:

Em se estabelecendo inovação como elemento transversal, é importante ter em mente que não se trata somente de um aspecto; não se deve ter em mente somente o desenvolvimento e o uso de novas tecnologias (como "big data", inteligência artificial e internet das coisas). Há pelo menos três aspectos de inovação que fazem sentido que sejam tomados em consideração: **(i) Inovação no uso de dados; (ii) Inovação em tecnologias; e (iii) Inovação em modelos de negócio.**

II) Sugestões de arranjos institucionais (*Hub de inovação*):

Em muitos projetos inovadores há uma porção de incerteza quanto ao modo

como as regulações se adaptam ao processo. Uma dessas questões se relaciona com a proteção de dados pessoais.

A autoridade de proteção de dados nesses casos deve considerar ter **órgãos internos especializados** que possam avaliar os riscos e as melhores formas de mitigação, representando um meio de dar maior clareza para a implementação de mecanismos de proteção de dados pessoais.

A autoridade do Reino Unido, por exemplo, possui uma subdivisão específica que está organizada para responder às dúvidas específicas de empresas e órgãos cujos projetos tenham aspectos inovadores relacionados a dados pessoais. O *Innovation Hub* da ICO trabalha em parceria com outros órgãos públicos para auxiliar a negócios em suas dúvidas e prestar suporte no que seja necessário para que a proteção de dados seja uma consideração constante no decorrer da empreitada.

Essa perspectiva faz com que seja possível que essas empresas (usualmente *startups*) possam dar vazão às suas obrigações de "***privacy by design***".

Ou seja, desde o início do processo de concepção e desenvolvimento de qualquer novo projeto possam pensar e tirar dúvidas sobre como melhor proteger dados pessoais.

O custo econômico e social tende a ser muito menor se houver uma ênfase em cuidados prévios do que em punição. Há além da mitigação dos riscos para dados pessoais, também ganhos relacionados aos acertos e aos novos bens e serviços a serem disponibilizados.

III) Sugestões de técnicas regulatórias (*regulatory sandboxes*):

Há uma preocupação estratégica com a possibilidade de uso de dados de maneiras novas e nunca pensadas antes. Por um lado, aparecem riscos atrelados a estas experimentações. Por outro, existem também grandes oportunidades.

As "*sandboxes regulatórias*" são ferramentas que permitem que sejam postas em prática inovações dentro e ambientes regulados e sob a supervisão de uma autoridade estatal reguladora. Há um aprendizado mútuo. O projeto pode se desenvolver e ser testado e a autoridade consegue visualizar de maneira mais direta os riscos e potenciais consequências (e inclusive interferir se necessário) das inovações.

O país já implementa esse tipo de técnica regulatória no campo das finanças de maneira que o Banco Central já estabeleceu uma normativa sobre o assunto e a CVM (Comissão de Valores Mobiliários) também.

Quanto à proteção de dados, esse tipo de técnica tem se mostrado efetiva. No Reino Unido, o Innovation Hub da ICO - mencionado acima - a utiliza já com sucesso (veja aqui e aqui). Uma organização sem fins lucrativos prestando serviços para o setor da educação foi o primeiro caso bem sucedido (Jisc). O segundo refere-se a automatização de parte dos processos da jornada dos passageiros no Aeroporto Heathrow.

Essas técnicas não precisam ser implementadas de maneira isolada, ao

contrário, pode ser relevante que **diferentes autoridades regulatórias atuem de maneira conjunta**. A autoridade de proteção de dados deve considerar instituir meios formais e informais de cooperação nesses casos.

CONCLUSÃO

É preciso considerar que a Lei Geral de Proteção de Dados pauta a atuação da Autoridade Nacional de Proteção de Dados e a aplicação de sanções administrativas em função da análise de risco e da consequente necessidade de se proteger o indivíduo.

Por consequente, é razoável que a aplicação da lei seja igualmente adequada ao grau do risco que as empresas representam. Nesse sentido, uma empresa que detém milhões de dados pessoais não pode ter o tratamento igual a uma empresa que mantém dezenas. Ademais, a natureza da atividade e a finalidade também são elementos importantes a serem considerados, a fim de não gerar onerosidade excessiva de modo a inviabilizar o próprio negócio das micro empresas.

A Lei Geral de Proteção de Dados deve, assim, ser compreendida como uma carta de proteção de direitos, mas também de oportunidades de negócio e não deve ser vista como obstáculo para inovação.

Esse relatório contou com o generoso apoio financeiro do Reino Unido através de programa *Digital Access*

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org