Opinião: Primeiras reflexões sobre a resolução CD/ANPD nº 2

O conselho diretor da Autoridade Nacional de Proteção de Dados (ANPD) publicou no último dia 28 a Resolução CD/ANPD nº 2, regulando o tratamento de dados pessoais por parte de agentes de tratamento de pequeno porte (microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito icroempreendedor individual).

A resolução faz parte do esforço da autoridade regulatória em endereçar normas e procedimentos simplificados aos agentes de tratamento classificados como de pequeno porte, com o intuito de facilitar a aplicação da LGPD por parte de tais agentes e proteger os dados pessoais dos titulares. A classificação como agente de tratamento de pequeno porte observa critérios de qualificação jurídica e os riscos do tratamento aos direitos dos titulares de dados.

Nesse sentido, cabe destacar que a resolução é um complemento ao "Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte", publicado em outubro de 2021.

Em que pese a importância da regulamentação, é importante analisar suas disposições sob dois aspectos: a) o que de fato foi flexibilizado ou dispensado; e b) se estrategicamente essa é a melhor opção para agentes de tratamento de pequeno porte.

Sob o primeiro aspecto, vejam-se os principais pontos flexibilizados pela resolução, para além do enquadramento como "agente de tratamento de pequeno porte":

1) Organização por meio de entidades de representação da atividade empresarial, por pessoas jurídicas ou por pessoas naturais para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares de dados;

A organização por meio de entidades de representação pode servir como uma forma de aperfeiçoar e articular os interesses desse segmento empresarial e servir como ponto de padronização de suas práticas e processos de gestão, facilitando, assim, a resposta aos interesses dos titulares de dados de forma mais estruturada e uniforme. Trata-se de um importante mecanismo para a construção de um ecossistema coeso e uniforme a respeito das regras a serem aplicadas por parte de tais agentes. Evidente que tais normas e procedimentos criados por agentes de tratamento de pequeno porte organizados em entidades representativas passarão pelo crivo da própria autoridade e da sociedade — ou pelo menos assim se espera.

2) Elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do artigo 37 da LGPD, de forma simplificada;

O registro das operações de tratamento de dados pessoais consiste em uma boa prática de governança, em que se específica, entre outras coisas, a forma pela qual se dá o tratamento dos dados pessoais, perpassando seu ciclo de vida (criação, uso, distribuição, armazenamento e exclusão). É um processo de catalogação do fluxo de dados pessoais objeto das operações de tratamento (artigo 5º, X), por meio de entrevistas diretamente com os responsáveis pelas áreas ou por formulários específicos — é o que comumente se chama de *data mapping*. Há, também, a atividade de identificação de quais dados são objeto de tratamento na empresa e onde estão armazenados, se internamente ou com terceiros externos.

Trata-se de um procedimento de difícil operacionalização e de elevado custo, pois envolve a necessidade de se aprofundar nos processos internos da empresa para ter um "retrato" assertivo dos fluxos de dados e dos tipos de dados tratados. Nesse sentido, a flexibilização dessa atividade, a princípio, foi algo bastante positivo. Cumpre destacar, todavia, que a ANPD ainda fornecerá o modelo para o citado registro simplificado, o que dificulta o planejamento para a incorporação dessa flexibilização.

De todo modo, recomenda-se que o registro seja feito da maneira mais robusta, quando possível, para que o agente de tratamento tenha ciência dos fluxos e dados tratados, obedecendo aos princípios da prevenção, transparência e responsabilização e prestação de contas da LGPD. Além disso, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, será considerada para fins de aplicação de sanções aos agentes de tratamento que descumprirem a lei (artigo 52, §1º, VIII).

3) Flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte (pendente de regulamentação);

Incidente de segurança com dados pessoais é qualquer situação de violação à segurança dos dados pessoais, desde acessos não autorizados a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O artigo 48 da LGPD determina que o controlador deverá comunicar à autoridade nacional e ao titular de dados a ocorrência de incidente de segurança que possa resultar em risco ou dano relevante aos titulares de dados.

Atualmente, a LGPD exige que sejam mencionados: 1) a descrição da natureza dos dados pessoais afetados; 2) as informações sobre os titulares envolvidos; 3) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; 4) os riscos relacionados ao incidente; 5) os motivos da demora, no caso de a comunicação não ter sido imediata; e 6) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD disponibiliza em seu site o formulário a ser preenchido, o qual deve ser enviado por meio de peticionamento eletrônico — usuário externo. Com exceção de algumas perguntas iniciais acerca do tipo de comunicação e para identificação do agente de tratamento, do notificante e do encarregado, o formulário contém apenas 17 perguntas, as quais se referem: ao incidente de segurança; às medidas de segurança utilizadas para a proteção dos dados; aos riscos relacionados ao incidente de segurança; e à comunicação aos titulares de dados. Trata-se, portanto, de um formulário já sucinto, adequado para contemplar o cenário do incidente, os afetados por ele, as consequências e os próximos passos. Ademais, o envio por meio do peticionamento eletrônico é um procedimento bastante simples e de fácil compreensão pelo usuário.

Dessa forma, faz-se necessário aguardar a regulamentação pela ANPD para verificar qual será a simplificação proposta pela Autoridade, tendo em vista que o atual formulário de comunicação de incidentes já é bastante adequado, mesmo à realidade dos agentes de tratamento de pequeno porte.

5) Desnecessidade de indicação de encarregado de dados;

A dispensa da nomeação do encarregado já era algo esperado para os agentes de tratamento de pequeno porte, até em função do artigo 41, §3º, que dispõe a respeito da regulamentação, por parte da ANPD, da exigência e dispensa desse profissional conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Embora os agentes de pequeno porte estejam desobrigados de nomear tal profissional, ainda assim devem fornecer um canal de comunicação que possibilite ao titular de dados exercer seus direitos e demandar da instituição informações a respeito do tratamento de seus dados. A nomeação do encarregado será considerada política de boas práticas e governança para os fins da aplicação de sanções.

Nesse sentido, conclui-se que, para efeitos de mitigação de riscos e dos custos de responsabilização em casos de vazamento de dados, a contratação desse profissional, ainda que de um *DPO as a service*, é algo a ser considerado pelos agentes de tratamento de pequeno porte, especialmente para atender aos chamados dos titulares de dados que certamente passarão a exercer seus direitos com mais frequência.

5) Estabelecimento de política simplificada de segurança da informação;

Embora tenha sido uma importante flexibilização, esse é um tema que deve ser visto com cautela. A Política de Segurança da Informação (PSI) tem por objetivo, entre outros, estabelecer diretrizes a serem seguidas pela empresa quanto aos aspectos da confidencialidade, disponibilidade e integridade e autenticidade dos dados e orientar a elaboração de normas específicas para a utilização segura dos ativos de informação da empresa.

A PSI deve ser adequada aos propósitos da organização, incluir os objetivos da segurança da informação (o que será feito; quais os recursos necessários; quem será o responsável; quando estará concluído; como os resultados serão avaliados), incluir o comprometimento em satisfazer os requisitos aplicáveis e o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

Trata-se, portanto, de um poderoso instrumento de gestão da segurança da informação para mitigar os riscos associados ao tratamento de dados e orientar os agentes de pequeno porte e seus colaboradores, além de servir como diferencial competitivo quando da contratação por agentes controladores que realizaram uma robusta adequação e procuram parceiros comerciais no mesmo nível de comprometimento. Nesse sentido, embora sua elaboração tenha sido flexibilizada pela Autoridade, é recomendado que agentes de tratamento de pequeno porte, especialmente aqueles com quantidade razoável de colaboradores, que invistam em conscientização para o fortalecimento da cultura da proteção de dados e segurança da informação.

6) Prazo em dobro para: a) atendimento das solicitações dos titulares de dados; b) comunicação à ANPD e ao titular da ocorrência de incidente de segurança; c) no fornecimento de declaração clara e completa quando da requisição do titular da confirmação e existência ou o acesso a dados pessoais; e d) em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

Com relação aos prazos diferenciados para os agentes de tratamento de pequeno porte, trata-se de uma relevante e positiva flexibilização.

Em primeiro lugar, uma vez que se tratam, como o próprio nome indica, de agentes de "pequeno porte", estes têm, em geral, uma estrutura pequena, com poucos funcionários. Em segundo lugar, diante da flexibilização quanto à obrigatoriedade de nomeação de um encarregado de dados, quem atenderá a demanda poderá não ser uma pessoa com conhecimento e experiência nessa área.

Dessa forma, o estabelecimento de um prazo maior é importante para que esses agentes possam cumprir as determinações da lei da melhor forma possível.

O que se pergunta, agora, é: estrategicamente, a opção pelo cumprimento flexibilizado das regras da LGPD é a melhor opção para agentes de tratamento de pequeno porte?

Entre os pontos destacados anteriormente, esses são, a nosso ver, os mais benéficos aos agentes de tratamento: 1) organização por meio de entidades de representação da atividade empresarial, considerando a possibilidade de padronização de certas práticas; 2) elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do artigo 37 da LGPD, de forma simplificada, tendo em vista o custo operacional e financeiro para a elaboração; 3) desnecessidade de indicação de encarregado de dados, em virtude do elevado custo de manutenção, embora existam plataformas de *DPO as a service* que podem ajudar nessa tarefa.

A 3), flexibilização ou procedimento simplificado de comunicação de incidente de segurança, e a 4), estabelecimento de política simplificada de segurança da informação, são pontos a serem vistos com certa cautela por parte de tais agentes, pois empresas mais robustas podem observar tal flexibilização como uma fragilidade e buscar parceiros que tenham investido um pouco mais em procedimentos técnicos e administrativos de cuidado e utilização de dados.

Nesse sentido, embora a resolução tenha buscado dispensar ou flexibilizar o cumprimento das normas da LGPD, ainda é prudente que os agentes de tratamento de pequeno porte procurem cumprir todas as determinações da lei, especialmente quando o tratamento puder ser considerado de alto risco, nos termos do artigo 4º. A própria classificação como sendo ou não de alto risco demandará uma análise mais detida das operações do agente de tratamento, considerando que há um certo grau de subjetividade na definição do tratamento *"em larga escala"* e que pode *"afetar significativamente interesses e direitos fundamentais"*. Além disso, considerando as circunstâncias relevantes da situação, como a natureza ou volume das operações, bem como os riscos para os titulares, a Autoridade poderá determinar que tais agentes cumpram todas as obrigações dispensadas. Assim, aqueles que querem se classificar como "agentes de tratamento de pequeno porte" devem avaliar com cuidado os requisitos dos artigos 2º e 3º da resolução.

Por fim, cumpre destacar que a dispensa ou flexibilização das obrigações do regulamento *"não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares ou contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares"* (artigo 6º da resolução). Isso significa que, não obstante as poucas flexibilizações, ainda permanece a obrigação de ter um controle sobre as principais tecnologias utilizadas, os locais de armazenamento dos dados, origem dos dados, compartilhamento com terceiros internos e externos à empresa ou com órgãos públicos, normas claras de retenção e exclusão de dados, procedimentos contratuais claros que especificam papéis e responsabilidades de controladores e operadores. Ou seja, os agentes de tratamento de pequeno porte devem cumprir toda a LGPD, exceto naquilo que foram expressamente dispensados.

Date Created
10/02/2022