

Contribuição à Consulta Pública sobre a Norma de aplicação da LGPD para microempresas e empresas de pequeno porte





Ficha técnica

Associação de Pesquisa Data Privacy Brasil

Direção: Bruno Bioni e Rafael Zanatta

Coordenação Geral de Projetos: Mariana Riell e Marina Meira

Data Privacy Brasil Ensino

Direção: Bruno Bioni e Renato Leite Monteiro

Coordenação Acadêmica: Pedro Bastos Lobo Martins

Coordenação de Comunicação: Victor Scarlato

Autores

Bruno Bioni

Rafael Zanatta

Pedro Bastos Lobo Martins

Hana Mesquita

Nathan Paschoalini

Paula Guedes Fernandes da Silva

Thaís Aguiar

Diagramação: Roberto Junior

Contribuição à Consulta Pública sobre a Norma de aplicação da LGPD para microempresas e empresas de pequeno porte

INTRODUÇÃO

A Autoridade Nacional de Proteção de Dados (ANPD) recebeu contribuições para a Consulta Pública sobre a norma de aplicação da LGPD para agentes de tratamento de pequeno porte. O Data Privacy Brasil, em sua missão de colaborar para o debate público sobre proteção de dados, submete a presente contribuição.

A contribuição foi feita a partir de um trabalho interinstitucional entre a Associação Data Privacy de Pesquisa e a Data Privacy Brasil Ensino. A partir da minuta proposta pela Autoridade Nacional, elencou-se sete principais pontos de atenção que merecem maior cuidado e aprofundamento por parte da ANPD.

1. Atividades de tratamento de alto risco

Considera-se acertada a abordagem adotada pela ANPD de considerar não só o porte econômico dos agentes de tratamento, mas também o risco aos titulares ocasionados pelas atividades de tratamento de dados. Contudo, acreditamos que o critério de larga escala não deve ser considerado um critério cumulativo ao alto risco, conforme se encontra atualmente na minuta proposta. Ao contrário, a larga escala é um critério para se considerar uma atividade de tratamento de dados como de alto risco.

2. Obrigação de registros das atividades de tratamento

A minuta de resolução proposta prevê a dispensa completa e um sistema de registro voluntário por parte de agentes de pequeno porte. Além de extrapolar as competências previstas no art. 55-J, XVIII e o disposto no art. 37 da LGPD, o registro das atividades de tratamento mostra-se como obrigação fundamental para uma adequada governança de atividades de tratamento de dados, materializando o princípio da responsabilização e prestação de contas.

3. Relatório de Impacto à Proteção de Dados Pessoais

A flexibilização do instrumento do relatório de impacto à proteção de dados pessoais encontra-se em desarmonia com a abordagem adotada pela ANPD na presente minuta de resolução. O instrumento do relatório de impacto não deve ter como parâmetro o porte do agente de tratamento, mas sim o risco de uma atividade ou de um conjunto de atividades de tratamento realizadas. Não há razão, portanto, em se flexibilizar uma obrigação que necessariamente nasce a partir de uma atividade de risco, critério este que afasta as flexibilizações trazidas pela presente proposta de resolução.

4. Segurança da Informação

Contudo, o elemento que deflagra esse dever é o **risco** ocasionado por esse incidente, nos termos do art. 48, caput da LGPD.

Assim, o porte do agente de tratamento não deve ser um elemento a se considerar para a dispensa ou flexibilização dessa obrigação. Nada impede, contudo, que procedimentos simplificados e facilitados sejam oferecidos a agentes de pequeno porte. Calibrar e flexibilizar o procedimento para essa comunicação não se confunde, em hipótese alguma, com uma flexibilização ou dispensa desse dever de comunicar.

Ainda, na criação de uma política de segurança simplificada para agentes de pequeno porte, é fundamental que a harmonia entre a LGPD e demais legislações seja preservada. Nesse sentido, recomenda-se que os padrões mínimos previstos no Marco Civil da Internet e em seu Decreto regulamentador (Decreto nº 8.771) sejam observados, em especial o estabelecimento de controle de acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso; previsão de mecanismos de autenticação; e gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

5. Indicação de Encarregado

Embora a opção pela dispensa de indicação de encarregado para agentes de pequeno porte possa ser adotada pela ANPD, deve-se considerar essa indicação como uma boa prática por parte dos agentes de tratamento, garantindo maior proteção aos direitos e liberdades fundamentais dos titulares de dados, o que deve

ser expressamente estipulado pela Autoridade Nacional de Proteção de Dados na futura resolução.

Ainda, com o intuito de mitigar os custos gerados pela indicação de um encarregado, a ANPD poderia prever também a possibilidade de nomeação de um mesmo encarregado por um conjunto de associações, fundações, microempresas, pequenos empresários e startups, quando reunidos em uma associação.

6. Prazos diferenciados

O artigo 16 da minuta proposta prevê a concessão de prazo em dobro para agentes de pequeno porte em algumas hipóteses, sendo uma delas a de comunicação de incidente de segurança, em seu inciso II. Nesse sentido, o dispositivo destacado aborda dois tipos de notificação: uma à Autoridade, outra aos titulares. Ainda que ambos se aproximem por buscarem sempre a limitação dos danos ocasionados pelo incidente, há diferenças notáveis quanto aos objetivos de cada comunicação e, portanto, em suas respectivas abordagens.

Além de cumprirem objetivos diferentes, as notificações também se dão de forma distinta, quando feita a um titular de dados e quando feita à Autoridade Nacional de Proteção de Dados. Ao contrário da comunicação aos titulares, não existem grandes empecilhos para identificar o canal de recebimento de comunicação e os meios pelo qual essa comunicação deva ser realizada. É possível ainda que, em regulamentação específica, a ANPD disponha sobre uma comunicação faseada de incidentes de segurança. Ou seja, caso o agente de tratamento tenha dificuldades de coletar todas as informações para uma comunicação completa para a Autoridade, ele poderia primeiro fazer uma comunicação simplificada e, em segundo momento, complementá-la com mais informações. Nesse sentido, a concessão de prazo em dobro para comunicar um incidente à ANPD mostra-se desproporcional, visto que esta poderia se dar de forma simplificada.

7. Direitos dos titulares

Embora as obrigações relativas ao atendimento de direito dos titulares possam ser simplificados para agentes de pequeno porte, a dispensa total do cumprimento de obrigações relativas a um direito previsto em lei mostra-se não só como ação que foge da competência de um ato administrativo, mas também como uma prática que vulnerabiliza ainda mais os titulares de dados.

Nesse sentido, recomendamos que a declaração clara e completa dos dados pessoais do titular, previsto pelo art. 19, inciso II, da LGPD, se mantenha como uma obrigação legal para os agentes de pequeno porte que podem, contudo, contar com um modelo simplificado a ser desenvolvido pela ANPD.

Da mesma forma, a dispensa total do direito de portabilidade se mostra inadequada e deve ser adaptada para cada realidade. Agentes de pequeno porte que atuam em setores e segmentos que já possuem padrões de interoperabilidade não devem contar com a mesma dispensa que agentes que atuam em setores que ainda não possuem esse desenvolvimento.

Por fim, recomendamos que os agentes de tratamento que não possuam meios para anonimizar dados pessoais, possam eliminar ou bloquear esses dados, ainda que o titular solicite a sua anonimização.

Espera-se que interpretações e consensos possam surgir a partir deste documento e dos diálogos possibilitados por ele.

1. Atividades de tratamento de alto risco

A minuta de resolução objeto de análise visa regulamentar o tratamento de dados pessoais realizado por agentes de pequeno porte no âmbito da Lei Geral de Proteção de Dados (LGPD). Em especial, o intuito principal da resolução é a de criar situações de dispensa ou flexibilização de obrigações para esses agentes de forma razoável e proporcional, evitando a imposição de barreiras de entrada para atores de pequeno porte, em simultâneo à proteção dos titulares de dados pessoais, em particular, de seus direitos e liberdades fundamentais.

Dito isso, para além das dispensas e flexibilizações de obrigações da LGPD específicas para agentes de pequeno porte, a criação, no art. 3º, de hipóteses de exceção à aplicação da resolução em casos de tratamento de dados de alto risco ou¹ em larga escala merece destaque especial como uma posição acertada tomada pela Autoridade Nacional de Proteção de Dados. Caso o abrandamento das regras de proteção de dados pessoais fosse aplicado de forma uniforme para todos os agentes de pequeno porte, poderíamos tornar a proteção dos titulares de dados enfraquecida e fragilizada,

¹ Falaremos ao longo deste documento sobre a necessidade de alteração do texto do art. 3º, caput e §4º, da minuta de Resolução, substituindo a conjunção “e” para “ou”.

especialmente no caso de grupos vulneráveis.

Isso porque o risco associado às atividades de tratamento de dados pessoais não decorre necessariamente do tamanho, porte econômico ou natureza jurídica da organização responsável, mas sim pelos possíveis riscos gerados aos titulares pela operação de tratamento de dados pessoais, considerando características específicas desta atividade no caso concreto, como tipo e volume de dados pessoais tratados, contexto e finalidade.

1.1. Hipóteses de não aplicação da resolução a agentes de pequeno porte

Dito isso, passadas as considerações iniciais, passaremos a analisar os critérios de enquadramento dos agentes de pequeno porte às regras da resolução. Nesse sentido, o art. 3º da minuta determina que a dispensa e a flexibilização das obrigações previstas na resolução não são aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares. Esta exceção ao regime de flexibilização de agentes de tratamento de pequeno porte é de grande importância e incorpora uma noção mais complexa e robusta de regulação responsiva, não se deixando guiar unicamente pelo porte econômico, mas também pelas atividades (e seus riscos) desenvolvidas pelos agentes de tratamento.

No entanto, com o intuito de maior proteção dos titulares de dados pessoais, é fundamental que a Autoridade considere a **incorporação do elemento de larga escala como um critério para caracterização de uma atividade de tratamento como de alto risco**. Tal mudança se faz necessária porque, por vezes, o tratamento de dados de alto risco por agentes de pequeno porte não necessariamente é também realizado em larga escala, o que permitiria que atividades de tratamento de alto risco sejam enquadradas nas regras de dispensas e flexibilizações da resolução.

Ainda, a ideia de tratamento de dados em larga escala é tratada por outras diretrizes internacionais como um elemento que eleva o risco da atividade de tratamento. Como se pode ver, na diretiva do Article 29 Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”, o tratamento de dados em larga escala é um dos critérios para se avaliar o risco gerado por uma atividade de tratamento². Ou seja, a larga escala e o alto risco não são elementos independentes e cumulativos, mas sim elementos interdependentes.

Consequentemente, caso a alteração do texto não seja considerada, os direitos e liberdades fundamentais dos titulares de dados são postos em situação de extrema fragilidade. Por exemplo,

²Article 29 Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

o tratamento de dados pessoais de crianças que frequentam uma determinada instituição religiosa estaria no âmbito de aplicação da resolução, já que, por mais que haja o tratamento de alto risco nos termos da minuta, não há a cumulação com o requisito de larga escala.

Da mesma forma, haveria margem para que uma atividade de tratamento de dados de milhões de titulares, com cruzamento de bases de dados, de longa duração e em grande extensão geográfica, feita por uma *startup*, não atingisse os requisitos da redação atual do art. 3º, caso não cumulasse as hipóteses previstas no §1º.

Além disso, é fundamental que a flexibilização de obrigações da LGPD para agentes de pequeno porte leve também em consideração o cenário em que a organização está inserida. Isso porque há o risco de que esses agentes sejam utilizados por grandes instituições, que fazem o tratamento de dados pessoais de elevado risco ou em larga escala, como instrumento para burlar as regras mais rígidas da lei, já que não se enquadram no regime de agente de pequeno porte.

Em outras palavras, há o risco potencial de que agentes de tratamento de médio ou grande porte repassem atividades de tratamento para parceiros comerciais ou outros membros de grupo econômico que se enquadrem como agentes de pequeno porte. Nesse caso, haveria um desvirtuamento da flexibilização e uma evasão regulatória. Consequentemente, como forma de evitar esse problema, sugerimos que as flexibilizações e dispensas não sejam aplicáveis a agentes de tratamento que façam parte de um grupo econômico com agentes de grande porte.

Por fim, reforça-se que ainda que as hipóteses previstas no art. 3º §1º sejam meramente exemplificativas, há um erro conceitual em separar alto risco e larga escala. A razão de ser de um regime especial para tratamentos de larga escala é justamente a elevação do risco dessa atividade.

Recomendação

Logo, para que a ANPD firme entendimento quanto a parametrização de uma regulação assimétrica no campo de proteção de dados, sem que eventuais flexibilizações ocasionem danos ou riscos aos direitos e liberdades fundamentais dos titulares de dados, é fundamental que, além do porte econômico do agente de tratamento de dados, seja observada também a variável do risco da atividade de tratamento, de forma **não cumulativa** com o critério de larga escala, sendo este um elemento que pode ser usado para caracterizar uma atividade como de alto risco, e não um elemento externo.

Art. 3º A dispensa e a flexibilização das obrigações previstas nesta resolução não são

aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de **alto risco para os titulares**, ressalvada a hipótese prevista no art. 13, Parágrafo único

§1º Para fins desta resolução, será considerado tratamento de alto risco para os titulares, entre outras hipóteses, o tratamento que envolva:

I - atividade de tratamento de dados em larga escala

II - dados sensíveis ou dados de grupos vulneráveis, incluindo crianças e adolescentes e idosos;

III - vigilância ou controle de zonas acessíveis ao público;

IV - uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; ou

V - tratamento automatizado de dados pessoais que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 2º O tratamento de dados será caracterizado como de larga escala quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

§ 3º Para fins deste artigo não será considerado tratamento de larga escala o tratamento de dados de funcionários ou para fins exclusivos de gestão administrativa do agente de tratamento de pequeno porte.

§ 4º A ANPD disponibilizará guias e orientações que auxiliem os agentes de tratamento de pequeno porte a avaliar se realizam tratamento com **alto risco**.

§ 5º A dispensa e a flexibilização das obrigações previstas nesta resolução também não se aplicam a agentes de tratamento de pequeno porte que façam parte de conglomerados ou grupos econômicos formados por agentes de tratamento de grande porte que realizem tratamento de alto risco para os titulares.

1.2. Definição de tratamento de dados de alto risco

A minuta de resolução em análise traz a definição de “tratamento de alto risco para os titulares” no § 1º do art. 3º, a partir de um rol exemplificativo que inclui o tratamento relacionado a: (i) dados sensíveis e de grupos vulneráveis (criança, adolescente e idosos); (ii) vigilância ou controle de zonas acessíveis ao público; (iii) uso de tecnologias emergentes que possam causar dano material ou moral aos titulares, incluindo discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; (iv) tratamento automatizado de dados pessoais, como o *profiling*.

Inicialmente, relevante ressaltar a opção acertada da Autoridade ao colocar o titular de dados como ponto central da análise dos riscos associados a determinada atividade de tratamento de dados pessoais. Isso porque, na análise de aplicabilidade flexibilizada ou não para agentes de pequeno porte das regras da LGPD de proteção de dados pessoais, operações que apresentam alto risco devem ser aquelas que podem impactar de forma significativa as liberdades civis e os direitos fundamentais dos titulares de dados³.

Além disso, cabe também parabenizar a escolha da ANPD pelo rol exemplificativo de atividades consideradas de alto risco para os titulares, o que está de acordo com orientações internacionais, a exemplo do considerando 75 e art. 35 (3) do GDPR e de orientações do Grupo de Trabalho do Artigo 29º para a Proteção de Dados (WP29)⁴. Tal opção foi extremamente positiva porque a análise de risco é dinâmica, tornando difícil a manutenção da atualidade de um rol taxativo, que poderia potencialmente deixar de lado algumas operações de tratamento simplesmente porque casos semelhantes não foram previamente mapeados e analisados ou, diante da constante e rápida evolução tecnológica, sequer existiam⁵.

Em outras palavras, podem existir operações de tratamento de alto risco que não estejam incluídas no rol de exemplos do §1º, mas que, ainda assim, impliquem riscos elevados aos titulares de dados, não devendo ser desconsiderados⁶. Ademais, a adoção de rol exemplificativo está alinhado com a ideia de regulação responsiva e dinâmica, de forma a garantir uma resposta regulatória coerente com a realidade prática, atentando-se às mudanças fáticas das operações e seus consequentes

³ Ibid. p. 264.

⁴ Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. WP 248 rev.01, última revisão em 4 out. 2017. Disponível em: <https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf>. p. 9-10.

⁵ GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 264.

⁶ Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. WP 248 rev.01, última revisão em 4 out. 2017. Disponível em: <https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf>. p. 9-10.

efeitos aos titulares dos dados.

Apesar de todos os pontos positivos inaugurados pela minuta de resolução da Autoridade no que tange ao rol exemplificativo de atividades de tratamento de alto risco, o que inclui, por exemplo, o tratamento de dados sensíveis ou dados de grupos vulneráveis, ainda é necessária a criação de uma definição mais clara de quem seria enquadrado como membro de grupo vulnerável para fins de interpretação da resolução.

O texto atual do art. 3º, § 1º, inciso I, menciona “grupos vulneráveis”, colocando crianças, adolescentes e idosos como exemplos desta categoria de pessoas. Apesar de ser bem-vinda a proteção adicional a esses grupos, o conceito de “grupos vulneráveis” não se encontra presente na LGPD, sendo importante conceituá-lo na resolução.

No direito internacional, especificamente no cenário europeu de proteção de dados pessoais, o WP29 entende que a condição de vulnerabilidade é definida a partir da ideia de desequilíbrio de poder entre os titulares de dados e o agente de tratamento, o que dificultaria, por exemplo, o exercício legítimo do consentimento e de direitos dos titulares, especialmente o direito de oposição⁷.

No mesmo sentido, a Autoridade de Proteção de Dados do Reino Unido (*Information Commissioner's Office - ICO*) entende que indivíduos devem ser considerados vulneráveis quando as circunstâncias do tratamento de dados pessoais podem restringir sua capacidade de consentir livremente ou de se opor ao processamento de seus dados pessoais, ou, ainda, de compreender suas implicações. Por esse entendimento, crianças são facilmente consideradas parte do grupo vulnerável, assim como idosos e indivíduos com certos tipos de deficiências⁸.

Porém, mesmo que alguns indivíduos não façam parte de um grupo notoriamente considerado como vulnerável, um desequilíbrio de poder entre o titular e o agente de tratamento pode também causar vulnerabilidade para fins de proteção de dados, como é o caso de empregados em relação aos empregadores. Este tipo de vulnerabilidade também pode surgir devido à situação financeira de um indivíduo, como ocorre na classificação de crédito, ou ao contexto específico do tratamento, a exemplo de pacientes recebendo cuidados médicos⁹.

No contexto europeu, dados relativos a condenações penais e infrações são classificados como “categorias especiais de dados” e, portanto, sensíveis, o que já se enquadraria no art. 3º, §1º,

⁷ Ibid. p. 12.

⁸ Information Commissioner's Office. When do we need to do a DPIA? Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when2>>.

⁹ Ibid.

inciso I da minuta de resolução. Porém, como a LGPD não trouxe expressamente o enquadramento desse tipo de dado como sensível, seria adequado que a ANPD os incluísse dentro da categoria de dados de grupos vulneráveis para os fins da presente resolução, uma vez que tem um grande potencial de gerar efeitos discriminatórios, deixando os titulares em posição de vulnerabilidade e assimetria de forças em relação ao agente de tratamento.

Recomendação

Desta forma, com fins de garantia de maior segurança jurídica para os agentes de pequeno porte regulados, para além da lista de exemplos de grupos vulneráveis, seria aconselhável a elaboração de uma definição não exaustiva do termo no art. 2º, nos moldes realizados pelo WP29 no contexto do GDPR, além de aumentar o rol de exemplos do art. 3º, §1º, inciso I.

Assim, a partir da ideia de desequilíbrio de poder, titulares de dados pertencentes a grupos vulneráveis poderiam incluir, por exemplo: (i) crianças e adolescentes; (ii) empregados; (iii) grupos mais vulneráveis da população que necessitem de proteção especial, como pessoas com doenças mentais, solicitantes de asilo, idosos, doentes, dentre outros; (iv) todos os casos em que possa ser identificado um desequilíbrio na relação entre o titular de dados e o agente de tratamento¹⁰.

CAPÍTULO II DAS DEFINIÇÕES

Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:

I - microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º da Lei Complementar nº 123, de 14 de dezembro de 2006;

II – startups: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou

¹⁰ Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. WP 248 rev.01, última revisão em 4 out. 2017. Disponível em: <https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf>. p. 12.

a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021;

III – pessoas jurídicas sem fins lucrativos: associações, fundações, organizações religiosas e partidos políticos;

IV – agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

V – zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.

VI - dados de titulares vulneráveis: dados pessoais de titulares em condição de hipervulnerabilidade em relação ao agente de tratamento, como crianças, adolescentes, idosos e pessoas com deficiência.

Parágrafo único. Para fins desta resolução, consideram-se, ainda, agentes de tratamento de pequeno porte, os que possuem receita bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.

Art. 3º A dispensa e a flexibilização das obrigações previstas nesta resolução não são aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 13, Parágrafo único.

§ 1º Para fins desta resolução, será considerado tratamento de alto risco para os titulares, entre outras hipóteses, o tratamento que envolva:

I - atividade de tratamento de dados em larga escala

II - dados sensíveis ou dados de titulares vulneráveis, incluindo dados de condenações criminais, além de dados de crianças e adolescentes, pessoas com deficiência, idosos e quaisquer outros que se enquadrem na definição do art. 2º, inciso VI;

III – vigilância ou controle de zonas acessíveis ao público;

IV – uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; ou

V – tratamento automatizado de dados pessoais que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

1.3. Atividades de tratamento de dados em larga escala

A minuta de resolução em análise traz a definição de tratamento de dados “em larga escala” no § 2º do art. 3º, considerando situações de tratamento que envolvam um número significativo de titulares, além do volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

Assim como ocorre no contexto europeu, a Autoridade optou por não trazer uma definição exata do termo “larga escala”, já que não seria possível fornecer um número preciso da quantidade de dados processados ou de pessoas afetadas que seria aplicável a todas as situações, pois o tratamento de dados pode ser extremamente contextual. Isso não exclui, porém, a possibilidade de que a Autoridade, ao longo de sua atuação, traga orientações mais específicas, até mesmo mais quantitativas, do que constitui “larga escala” em relação a certos tipos de atividades de tratamento comuns, o que poderá ser feito de acordo com as práticas-padrão do mercado¹¹.

Dito isso, é positivo que a ANPD tenha definido, pelo menos, diretrizes mínimas para a classificação de tratamento de dados em “larga escala”, o que deve envolver um número significativo de titulares e volume de dados, assim como a duração, a frequência e a extensão geográfica do tratamento realizado. Neste ponto, é necessária uma maior definição do que a Autoridade entende como “número significativo de titulares”, seja como um número específico ou como uma proporção relevante da população, além da definição de situações exemplificadoras do tratamento em larga escala.

De acordo com o WP29, que está em sintonia com o considerando 91 do GDPR¹², exemplos

¹¹ Article 29 Working Party. Guidelines on Data Protection Officers (‘DPOs’). WP 243 rev.01, adotado em 13 dez. 2016.p. 7-8.

¹² Considerando 91 do GDPR: “(91) Tal deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos.

Dever-se-á realizar também uma avaliação de impacto sobre a proteção de dados nos casos em que os dados pessoais são tratados para tomar decisões relativas a determinadas pessoas singulares na sequência de qualquer avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas.

É igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controlo de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrónicos, ou para quaisquer outras operações quando a autoridade de controlo competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala.

O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado.

Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória.”

não exaustivos de tratamento de dados em larga escala incluem¹³:

- tratamento de dados de pacientes no curso normal dos negócios por um hospital (não por um médico individual);
- 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);
- tratamento de dados de geolocalização em tempo real de clientes de uma cadeia internacional de *fast food* para fins estatísticos por um agente especializado na prestação desses serviços;
- tratamento de dados de clientes no curso normal dos negócios por uma seguradora ou banco;
- tratamento de dados pessoais para publicidade comportamental por um mecanismo de pesquisa;
- tratamento de dados (conteúdo, tráfego, localização) por provedores de serviços de telefone ou internet.

Nesse sentido, é possível concluir, por exemplo, que não seria enquadrado como tratamento de dados em larga escala no caso de profissionais que processam dados de pacientes ou clientes, como acontece com advogados e médicos individuais¹⁴.

Outro ponto fundamental para a definição de larga escala está relacionado ao risco de que agentes de pequeno porte e organizações sem fins lucrativos tenham acesso ou façam uso compartilhado de bases de dados de grande escala, como, por exemplo, no caso de uso compartilhado de bases de dados do poder público no âmbito de contratos, convênios ou instrumentos congêneres com instituições públicas. Nesse caso, o tratamento de dados pessoais realizados por agentes de tratamento de pequeno porte deve ser considerado tratamento em larga escala, afastando as dispensas e flexibilizações da resolução em análise.

Recomendação

Para que a resolução de dispensas e flexibilizações de regras da LGPD para agentes de pequeno porte possa garantir a proteção efetiva de direitos e liberdades fundamentais dos titulares de dados, é fundamental que a Autoridade Nacional afaste de forma expressa as flexibilizações para atividades de tratamento que envolvam um grandes volumes de dados

¹³ Article 29 Working Party. Guidelines on Data Protection Officers ('DPOs'). WP 243 rev.01, adotado em 13 dez. 2016. p. 8.

¹⁴ Ibid. p. 8.

peçoais, o que seria classificado como uma espécie de tratamento de dados peçoais em larga escala, e, portanto, conforme argumentado anteriormente, uma atividade de alto risco.

Muitas dessas situações de tratamento em larga escala pode se dar por organizações de pequeno porte, que não tenham uma grande base de dados ou uma escala muito grande, porém, em razão de alguma parceria, convênio, contrato ou acordo, possam ter acesso a grandes bases de dados, especialmente bases de dados do poder público. Recomendamos que essas situações atraiam para si o regime geral da LGPD.

1.4. Publicação de guias e orientações sobre o tratamento de dados com alto risco ou em larga escala

Diante das pontuações elaboradas nos tópicos anteriores, a ANPD também acerta ao comprometer-se com a criação e consequente disponibilização de guias e orientações que auxiliem os agentes de tratamento de pequeno porte a avaliar se realizam tratamento com alto risco ou em larga escala, de acordo com o § 4º do art. 3º.

Nesta oportunidade, será essencial que a Autoridade especifique a metodologia científica de avaliação de risco que irá considerar, inclusive, a partir de exemplos da aplicação desses métodos em estudos de caso. Desta forma, é possível obter uma análise mais concreta de quais operações apresentam alto risco, orientando os regulados de pequeno porte de maneira mais clara e objetiva¹⁵.

A criação de diretrizes de avaliação de risco por parte da ANPD, baseadas em métodos e procedimentos científicos, que auxiliem aos agentes de pequeno porte a entender o grau de risco de suas atividades de tratamento é bem-vinda, pois auxiliará na promoção de maior segurança jurídica. Nesse âmbito, é recomendável que o risco possa ser mensurável a partir de indicadores previamente definidos, em diferentes níveis qualitativos, como alto, médio e baixo, afastando a classificação meramente quantitativa¹⁶.

Ademais, como mencionado anteriormente, é recomendável que a Autoridade traga alguns exemplos de situações de tratamento de dados por agentes de pequeno porte que sejam consideradas em larga escala, assim como realizada por outras autoridades de proteção de dados no contexto internacional, como o ICO do Reino Unido e o WP29 na União Europeia.

¹⁵ GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In.: Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 264.

¹⁶ Ibid. p. 262-265.

1.5. Organizações religiosas e partidos políticos como agentes de tratamento de pequeno porte

Ao fazermos uma interpretação conjunta do art. 2º, inciso III e IV, da minuta de resolução da ANPD, organizações religiosas e partidos políticos configuram como uma espécie de agente de tratamento de pequeno porte, o que poderia dispensar ou flexibilizar esses agentes de certas obrigações de proteção de dados previstas na LGPD.

Porém, tal opção pode se revelar problemática para os direitos e liberdades fundamentais dos titulares de dados, pois o tratamento de dados pessoais por instituições religiosas e partidos políticos é, em regra, sensível, já que lidam com informações relativas a convicção religiosa/filiação a organização de caráter religioso e opinião política/filiação a organização de caráter político, respectivamente, que constam da definição de dado pessoal sensível do art. 5º, inciso II da LGPD. Diante da sensibilidade originária dos tratamentos de dados pessoais feitos por essas organizações, é incongruente classificá-las como agentes de tratamento de pequeno porte, pois se enquadram, desde logo, na hipótese de tratamento de alto risco do art. 3º, §1º, inciso I.

Especificamente sobre instituições religiosas, no contexto europeu, não há norma específica que exclua essas organizações de regulações de proteção de dados¹⁷, como ocorreria pelo atual texto da resolução em análise. Pelo contrário, além da aplicação do regulamento, alguns Estados-Membros possuem também legislações específicas para o tratamento de dados pessoais por instituições religiosas, desde que estejam de acordo com as regras gerais do GDPR, como a sujeição à supervisão de uma autoridade supervisora independente (art. 91). Ainda, o Tribunal de Justiça da União Europeia já possui decisão firmada em que considerou tanto entidades religiosas quanto seus pregadores como controladores de dados, possuindo assim obrigação de cumprir as regras e princípios de proteção de dados¹⁸.

Quanto aos partidos políticos, as legislações de proteção de dados do contexto europeu são também completamente aplicáveis, principalmente após os escândalos de manipulação de processos eleitorais por meio do uso de dados pessoais, a exemplo do caso *Cambridge Analytica*. Autoridades de proteção de dados têm, inclusive, dado atenção especial ao tratamento de dados feito por partidos políticos, emitindo guias e recomendações específicos para esse contexto, por se tratar de uma atividade de grande relevância não só para a proteção dos titulares, mas de todo

¹⁷ BUTTARELLI, Giovanni. Personal Data Protection in churches and religious organisation Speech to a Conference organised by the Polish Inspector for Personal Data Protection, Cardinal Stefan Wyszyński University of Warsaw, Opole University and the University of Szczecin. Varsóvia, 25 fev. 2016. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/16-02-25_personal_data_protection_church_warsaw_en.pdf>.

¹⁸ Julgamento de Testemunhas de Jeová, C-25/17, ECLI:EU:C:2018:551. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=en>>.

sistema eleitoral e democrático¹⁹.

Todavia, caso a ANPD entenda que a inclusão de entidades religiosas e partidos políticos nas normas de flexibilização poderia se dar para atividades que não envolvam alto risco, deveria-se adotar uma abordagem em que as flexibilizações se dão com base em cada atividade de tratamento, e não com base no risco das atividades desenvolvidas pelo agente de forma geral, replicando a abordagem também para os demais agentes de tratamento.

Recomendação

Recomendamos a remoção da inclusão de partidos políticos e entidades religiosas como pessoas jurídicas sem fins lucrativos para os fins da resolução da presente resolução de flexibilização, visto que são entidades que necessariamente realizam tratamento de dados sensíveis, o que automaticamente as exclui pelo critério disposto no art. 3º, §1º, I.

Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:

III - pessoas jurídicas sem fins lucrativos: associações e fundações;

2. Obrigação de registro de atividade de tratamento

A intenção da ANPD de calibrar a amplitude da obrigação legal constante no art. 37 da LGPD é necessária para fins de segurança jurídica e equilíbrio econômico-regulatório, mas considerando a importância do registro de atividades de tratamento, não deveria ser imposta uma dispensa de plano, tampouco conferir a opção pelo registro voluntário, especialmente por não existir base jurídica para essa dispensa.

Conforme apontado pela Autoridade no Relatório de Análise de Impacto Regulatório, o GDPR prevê uma exceção para o registro de atividade para empresas que possuam menos de 250 funcionários, as quais não precisam manter registros do procedimento de tratamento de dados da mesma

¹⁹ INFORMATION COMMISSIONER'S OFFICE - UK political parties must improve data protection practices. 11 de novembro de 2020. Disponível em: <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/uk-political-parties-must-improve-data-protection-practices/>>; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Guidance for federal political parties on protecting personal information. 1 de abril de 2019. Disponível em: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904>.

forma que outras empresas²⁰. A obrigação apenas não é afastada em três casos: quando os tratamentos realizados tenham alto potencial de resultar em um risco para os direitos e liberdades dos titulares, quando eles forem tratamentos habituais ou, por fim, quando incluam dados de categoria especial ou dados relacionados a ofensas e condenações criminais.

Embora esta dispensa esteja consagrada na legislação europeia, recomenda-se que a ANPD não siga no mesmo caminho do Regulamento Europeu em razão dos motivos apresentados a seguir:

2.1. Competência legal para dispensar obrigações previstas em lei

A Lei Geral de Proteção de Dados prevê em seu art. 55-J a competência da Autoridade Nacional de proteção de Dados, e, dentre elas, está a de prever procedimentos simplificados e diferenciados para agentes de pequeno porte:

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

Como se pode observar, o art. 55-J, XVIII não garante à ANPD a competência para dispensar uma obrigação legal, o que é o caso da obrigação de registro de atividades de tratamento, previsto de forma taxativa pelo art. 37 da LGPD.

Ao contrário da hipótese prevista no art. 41, §3º, em que a dispensa de indicação do encarregado é prevista como uma prerrogativa da Autoridade Nacional, o art. 37 não traz a mesma abertura. Sendo assim, a Autoridade estaria agindo além de suas competências legais caso disponha sobre uma dispensa total.

De todo modo, acreditamos que a obrigação de registro de atividades de tratamento mostra-se como um dever importante não só por estar previsto em lei, mas por trazer benefícios concretos tanto aos agentes de tratamento quanto para os titulares de dados. Reconhece-se, contudo, que essa obrigação pode ser simplificada para agentes de pequeno porte, conforme será argumentado a seguir.

²⁰ Art. 30(5). The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

2.2. *Compliance e governança de dados: a Lei Geral de Proteção de Dados como uma janela de oportunidade para organização institucional e promoção da cultura de proteção de dados*

A dispensa total vai contra a lógica de construir uma cultura de proteção de dados no país, uma vez que se cria incentivos para que os agentes não cumpram as obrigações previstas pela LGPD, ou, ao menos, não registrem as suas decisões. Em um cenário de formação inicial isso é muito prejudicial. O incentivo deveria ser o oposto, de facilitar e promover que os agentes elaborem os registros de modo a desenvolver maturidade em matéria de proteção de dados e privacidade.

Nesse sentido, a obrigação de registro, embora possa ser onerosa a princípio, pode também ser entendida como um incentivo para que os agentes se organizem. A adequação à LGPD é mais do que somente uma obrigação legal - é uma janela de oportunidade para:

- Criação de novos produtos e revisão de modelo de negócio ou política pública;
- Análise dinâmica centrada no que a organização pode gerar de valor;
- Gestão baseada em inovação;
- reputação com base em dar mais transparência ao uso dos dados;
- Estímulo à inovação e competitividade o que, em última análise, favorece a reputação da organização

Conforme leciona Bruno Bioni, a LGPD obriga as organizações a “colocar ordem na casa” uma vez que será necessário conhecer as suas bases de dados e lhes atribuir uma finalidade específica - um dos princípios da lei²¹. No bojo de um projeto de adequação, é possível rever processos e compreender melhor o fluxo de dados da organização de modo a tornar o negócio mais eficiente. No aspecto reputacional, a transparência no tratamento de dados pessoais é um elemento valioso que pode ser explorado numa estratégia comercial e de marketing para fortalecer a relação com o titular de dados, trabalhando ainda a confiança no produto ou serviço oferecido.

O *compliance* de dados pessoais volta-se justamente para auxiliar os agentes de tratamento a aplicar de forma eficaz as normas de proteção de dados, permitindo que o agente mantenha esses dados e toda a sua atividade dentro dos ditames legais, utilizando a segurança da informação em prol da minimização de incidentes que implique em responsabilização. O registro também é um pilar de qualquer programa de conformidade com a LGPD, independente da sua dimensão ou forma e, inclusive, é próximo do processo de mapeamento de dados que faz parte do diagnóstico que todas as entidades devem realizar sob a LGPD. Nesse sentido:

²¹ BIONI, Bruno. Inovar pela Lei. A Era dos Dados. Disponível em: <https://brunobioni.com.br/home/wp-content/uploads/2019/08/gv_0184ce5.pdf>. Acessado em 10 de setembro de 2021. GV- Executivo • Vol. 18 • nº 4 • Julho/Agosto de 2019.

“Apenas a partir da concreta identificação das necessidades específicas de adaptação de cada agente é possível garantir a conformidade com a LGPD. (...) Além de garantir a conformidade com as demais normas da LGPD, os agentes de tratamento devem construir estruturas que permitam o atendimento a diversos outros deveres específicos, associados a boas práticas corporativas. *É o caso do dever de manter registro de todas as atividades de tratamento realizadas* (art. 37)”²² (grifou-se)

O registro de atividades de tratamento é a base de qualquer programa de governança de dados. Sem essa fotografia é praticamente impossível (ou extremamente difícil) identificar os fluxos de dados, bem como as eventuais lacunas (“gaps”), as recomendações e as alterações que devem ser realizadas com vistas à adequação. É o “esqueleto” do programa de governança, sendo um documento fundamental independentemente do porte da organização. É o diário, inventário ou livro contábil das operações de tratamento.

Conforme aponta o Centre for Information Policy Leadership:

*“As organizações de todos os tipos, tamanhos, culturas corporativas, setores podem desenvolver e implementar programas de governança da privacidade e proteção de dados pessoais adequados a seu contexto, riscos e objetivos específicos. Embora possa ser mais desafiador para as PMEs implementar um programa completo, elas também podem adotar medidas para organizar e estruturar seus esforços de governança de privacidade e proteção de dados, muitas vezes de forma mais ágil do que organizações maiores, dependendo dos tipos de dados pessoais que tratam.”*²³

Os próprios agentes de tratamento devem desenvolver suas técnicas e metodologias para o registro, adaptados ao seu contexto e capacidades, em uma lógica de regulação responsiva.

2.3. Necessidade de conferir concretude a determinados preceitos da lei

Além de representar a espinha dorsal de qualquer projeto de adequação, o registro é uma forma de concretizar determinados princípios da Lei como transparência, prestação de contas e

22 FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. O compliance de dados pessoais. In. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Coord. Ana Frazão, Gustavo Tepedino e Milena Donato Oliva. Revista dos Tribunais. Julho 2019. p. 698.

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

minimização de dados, sendo ainda um meio de facilitar o exercício dos direitos do titular.

No tocante à transparência e prestação de contas, o registro é instrumento importante, senão essencial, para a garantia de prestação de contas na medida em que a documentação deve estar apta a demonstrar, no mínimo, os fluxos (internos e externos) de tratamento de dados e a sua gestão.

No Relatório de Análise de Impacto Regulatório, a ANPD acertadamente reconheceu que:

“Manter o registro das atividades de tratamento, por outro lado, é importante para conferir segurança jurídica tanto a esse grupo de agentes de tratamento, quanto ao titular de dados, além de atender aos comandos da transparência, de accountability e do acesso aos dados pelo titular. Ainda que não mantidos os registros das atividades de tratamento de dados pessoais, é importante que as organizações conheçam o ciclo de vida dos dados, como e quais dados coleta e que atividades de tratamento realizam.”

Além de facilitar a materialização do princípio da accountability, a criação de registros das atividades de tratamento de dados facilita o exercício dos direitos dos titulares (especialmente do art. 18). Cita-se, por exemplo, o direito à “informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados” (art. 18, VII), elemento que compõe, justamente, o fluxo dos dados pessoais. Desse modo, o registro facilita a identificação das operações e dos dados pessoais tratados de modo a tornar mais eficiente a resposta à solicitação do titular (valorização da transparência na relação com o titular). O sistema de tratamento deve permitir o pleno exercício dos direitos dos titulares.

2.4. Necessidade de conferir concretude a determinados preceitos da lei

Além disso, a elaboração e manutenção do registro permite identificar a que título se realiza o tratamento de dados – como operador ou como controlador. Isso é fundamental na medida em que afeta os deveres e o grau de responsabilidade do agente quando da ocorrência de um dano (arts. 42 a 46 da LGPD). Sem o registro, a atribuição dos papéis e responsabilidades dos agentes envolvidos torna-se uma tarefa ainda mais difícil, haja vista que o documento facilita a visualização dos fluxos de dados e, conseqüentemente, das partes afetadas pelo tratamento.

2.5. Identificação de riscos e revisão de processos

A criação e atualização do registro são ocasiões para identificar e hierarquizar os riscos de processamento à luz da LGPD. Esta etapa essencial permite que o agente de tratamento trace um plano

de ação do processamento em conformidade com as regras de proteção de dados. O importante é mapear todo o ciclo de dados e suas principais características, já que são inúmeros os fatores que podem influenciar no nível de risco.

Conforme estabelece o documento “Orientações relativas à aplicação do Regulamento Geral sobre Proteção de Dados a partir de 25 de maio de 2018”:

“É importante que os responsáveis pelo tratamento e os subcontratantes realizem revisões rigorosas aos respectivos ciclos da política de dados, de forma a identificarem claramente quais os dados que devem ser conservados, para que fins e que base é aplicável.”

Nesse sentido, o registro de operações de tratamento de dados é a peça-chave na avaliação dos riscos e não deve ser dispensado de plano em razão do porte do agente de tratamento. Assim, a flexibilização da obrigação de manter o registro de operação de tratamento deve convergir fortemente os critérios de porte/capacidade econômica e risco atrelado à atividade do agente econômico em questão.

Existem agentes de tratamento de pequeno porte que lidam com um volume enorme de dados e desempenham operações de tratamento altamente complexas, o que reforça a necessidade de manutenção de um registro. A parametrização de uma regulação assimétrica para distintos atores econômicos deve se pautar (não exclusivamente, mas principalmente) em uma análise sobre o risco que as suas atividades de tratamento de dados implicam para os titulares. Não significa dizer que o porte econômico da organização não deva ser levado em consideração (na medida em que isso pode afetar sua capacidade efetiva de estar em conformidade com determinadas previsões), mas que a ele deve se aliar a análise de risco, que pode incluir variáveis como modelo de negócio e atividades específicas de tratamento de dados, que se desdobram, por sua vez, em critérios como a existência de tratamento de dados sensíveis, tomada de decisão automatizada, profiling, bem como o volume de dados tratados.

Conforme mencionado anteriormente, o Art. 30, GDPR, dispensa para empresas com menos de 250 empregados, ressalvadas aquelas com menos de 250 se: (1) o tratamento que realiza puder resultar em risco para os direitos e liberdades dos titulares dos dados; (2) o processamento não for ocasional; (3) o processamento incluir categorias especiais de dados pessoais e (4) o processamento incluir dados pessoais relativos a condenações criminais e infrações. Portanto, pela legislação europeia, não faria sentido dispensar totalmente os agentes de pequeno porte de plano a partir de um critério quantitativo de funcionários, mas sim calibrar de acordo com a natureza e volume dos dados tratados.

É importante destacar que são as atividades de tratamento desenvolvidas e as eventuais operações que envolvam compartilhamento e transferência de dados que irão ditar a complexidade e extensão do registro, sendo ele uma "fotografia em série"²⁴ das operações de tratamento de dados em curso e do seu status jurídico e de segurança da informação.

2.6. O registro de operações de tratamento e as bases legais

A dispensa se torna ainda mais grave na hipótese na qual a base legal atribuída é o **legítimo interesse** ou quando o tratamento envolver **dados sensíveis ou de titulares vulneráveis**, tais como crianças, adolescentes e idosos. A base do legítimo interesse pode vir a ser amplamente utilizada, principalmente por empresas emergentes de tecnologia, tais como *startups*.

O legítimo interesse é uma base legal que exige um cuidado diferenciado uma vez que é necessário documentar a escolha por essa base, bem como justificá-la por meio do teste de legítimo interesse. O registro é, portanto, necessário para todo o tratamento empreendido, mas merece destaque no caso de operações justificadas com base no legítimo interesse do controlador – que devem contemplar informações ainda mais detalhadas²⁵.

Em um segundo exemplo, o consentimento enquanto base legal requer uma série de condicionantes para que seja considerado um consentimento lícito. Dentre eles, a demonstração de que foi dado de forma livre, informada, inequívoca e para uma finalidade determinada (art. 5º, XII). A LGPD prevê ainda que cabe ao controlador o ônus de demonstrar que esse consentimento foi obtido em conformidade com o disposto na lei²⁶. Sem um registro, torna-se impossível essa demonstração.

Por fim, outro exemplo da importância da obrigação de registro das atividades de tratamento ocorre no caso de incidentes de segurança, mesmo quando as circunstâncias do caso concreto não obrigam a comunicação para a ANPD. Assim, ainda que não haja a obrigação de notificação do incidente, é fundamental que o controlador registre a ocorrência do incidente considerado irrelevante e as razões para classificá-lo dessa forma, inclusive como boa prática de prestação de contas, como será mais bem explicado em tópico específico de segurança da informação.

²⁴ BIONI, Bruno. A obrigação de registro das atividades de tratamento de dados. Disponível em: <<https://genjuridico.jusbrasil.com.br/artigos/749546931/a-obrigacao-de-registro-das-atividades-de-tratamento-de-dados>>. Acessado em 21 de setembro de 2021.

²⁵ FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. O compliance de dados pessoais. In. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Coord. Ana Frazão, Gustavo Tepedino e Milena Donato Oliva. Revista dos Tribunais. Julho 2019. p. 703.

²⁶ Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

Recomendação

Um modelo de registro simplificados atende à preocupação manifestada pela ANPD no Relatório de Análise de Impacto Regulatório no qual destacou-se que “o pequeno volume de dados envolvido nas atividades das microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, o registro torna-se uma exigência desproporcional em razão do custo envolvido, seja em termos de capacitação jurídica e técnica, seja em termos financeiros para manutenção contínua dessa atividade”.

Nesse contexto, os desafios técnicos e financeiros podem ser satisfatoriamente superados mediante a disponibilização de modelos de registros mais simples e de fácil compreensão e usabilidade, sem os prejuízos e preocupações levantadas acima.

Art. 10. Os agentes de tratamento de pequeno porte **deverão** elaborar e manter os registros das operações de tratamento de dados pessoais constante do art. 37 da LGPD.

Parágrafo único. A ANPD fornecerá modelos para o **registro simplificado** das atividades de tratamento por agentes de tratamento de pequeno porte.

3. Relatório de Impacto à Proteção de Dados Pessoais

No que diz respeito à proposta de flexibilização na condução de Relatórios de Impacto à Proteção de Dados (RIPD), existe um conflito preliminar que representa uma contradição fundamental e que deve ser considerada para a presente contribuição. Tal contradição reside, justamente, no fato de esta minuta, proposta pela Autoridade Nacional de Proteção de Dados (ANPD), definir o seu escopo de abrangência como sendo direcionado às organizações de pequeno porte que não realizam tratamentos de alto risco, conforme é possível se extrair de uma leitura sistemática dos arts. 1º e 3º, caput. Desse modo, exclui-se os agentes que conduzem processos de tratamentos adjetivados com a característica fundamental e essencial para elaboração de Relatório de Impacto, qual seja, o elevado grau de risco para os titulares de dados.

Feitas tais considerações preliminares, destaca-se que a Lei Geral de Proteção de Dados (LGPD), ao estabelecer um instrumento como o Relatório de Impacto à Proteção de Dados, atribui à noção de risco um papel protagonista nas dinâmicas de proteção de dados pessoais, de modo que é possível estabelecer um diálogo com o processo mais geral e observável de “risquificação” das leis de proteção de dados pessoais, considerando que tais legislações foram desenvolvidas com intuito de

regular e mitigar os possíveis riscos decorrentes do desenvolvimento de tecnologias da informação e comunicação, além de garantir a proteção dos direitos fundamentais dos indivíduos²⁷.

Desse modo, esta contribuição caminha no sentido de advogar pelo estabelecimento de uma regulação responsiva ao risco, buscando estabelecer uma abordagem sistemática, a partir de contribuições anteriores feitas pelo Data Privacy Brasil. Significa dizer que defendemos uma regulação cuja aplicação deva ser tão rígida quanto os riscos gerados pela atividade de tratamento de dados pessoais. Sendo tais riscos compreendidos como possíveis danos aos titulares dos dados, seja sob uma perspectiva individual ou sistêmica.

Nesse sentido, é possível dizer que a natureza do relatório de impacto se relaciona com uma lógica de prevenção, ainda que a LGPD tenha priorizado a mitigação de riscos²⁸ em sua redação. Portanto, o RIPD cumpre o papel de “[...] ser uma ferramenta de governança de dados a ser internalizada no cotidiano da organização, não apenas um documento para ser utilizado durante um processo de adequação regulatória”²⁹.

No entanto, ao tornar a compreensão de risco como balizadora para o sistema de proteção de dados pessoais e mais especificamente para a elaboração de relatórios de impacto à proteção de dados, surgem questionamentos acerca de sua conceituação, pois que a LGPD, acertadamente, se furtou de estabelecer definições sobre o que seria risco ou sobre quais as atividades ensejariam um alto grau de risco para os titulares de dados, considerando que uma compreensão equivocada de risco geraria tanto consequências sancionatórias aos agentes de tratamento quanto aos titulares de dados³⁰.

Ao adotar uma abordagem meta regulatória, na qual agentes reguladores e agentes regulados cumprem papéis importantes para o ecossistema de proteção de dados pessoais, acrescido o fato de a ANPD ainda estar iniciando o seu processo regulatório, a avaliação de risco se transformou, tão somente, em uma tarefa para demonstrar conformidade com a Lei Geral de Proteção de Dados, de modo a estar mais orientado para um risco regulatório (de conformidade) da organização, do que para o trato dos possíveis riscos aos titulares de dados³¹.

27 QUELLE, C. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? Tilburg Law School Research Paper , 1-36, 20.

28 GOMES, Maria Cecília Oliveira. Relatório de Impacto à Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD. Revista do Advogado, v. 39, n. 144, 2019.

29 Ibid, p. 12.

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

31 Ibid p. 13.

Tais considerações são importantes, na medida em que revelam tanto a complexidade quanto às dificuldades relacionadas ao processo regulatório da ferramenta do Relatório de Impacto à Proteção de Dados. A complexidade regulatória é, portanto, reflexo da própria complexidade do instrumento-processo aqui em análise, como pode-se depreender da leitura do artigo 5º, inciso XVIII, da Lei Geral de Proteção de Dados, que define o RIPD como um documento do controlador em que deve haver a descrição dos processos de tratamento de dados que representem elevado grau de risco às liberdades civis e direitos fundamentais dos titulares de dados³², bem como deve conter o estabelecimento de medidas, salvaguardas e mecanismos de mitigação de risco.

Dessa forma, reitera-se que o risco que tornaria necessária a elaboração do Relatório de Impacto é aquele atrelado à condução de atividades de tratamento que possam representar elevado grau de risco para os direitos fundamentais e liberdades individuais dos titulares de dados, não havendo qualquer relação necessária com o porte econômico do agente de tratamento. A consideração do porte do agente de tratamento revela, portanto, uma confusão conceitual sobre o que de fato é o Relatório de Impacto à Proteção de Dados Pessoais. Tal impossibilidade de se excepcionar a condução do RIPD por agentes de tratamento, em razão de sua estrutura econômica, também foi reconhecida pelo Relatório de Análise de Impacto Regulatório sobre a construção de normas específicas para organizações de pequeno porte, publicado pela Autoridade Nacional de Proteção de Dados, em agosto deste ano³³.

Uma outra questão que nos parece relevante é o fato de o instrumento aqui em análise ainda estar em processo de regulamentação pela ANPD, considerando o disposto na Agenda Regulatória desta Autoridade para o Biênio 2021-2022, de modo que ainda não foram estabelecidas normatizações mínimas acerca de sua elaboração, o que dificultaria o processo de simplificação proposto pela presente minuta. Do mesmo modo, tal preocupação foi aventada pela Autoridade Nacional de Proteção de Dados no já citado Relatório de Análise de Impacto Regulatório:

32 Segundo o considerando nº 75 do Regulamento Geral de Proteção de Dados da União Europeia, o risco para direitos e liberdades dos titulares, "(...) cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados"

33 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Análise de Impacto Regulatório: construção do modelo regulatório para aplicação da LGPD a microempresas e empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais. Brasília, 2021.

Se por um lado a inclusão da simplificação em norma única favorece esse grupo de agentes de tratamento ao desonerá-los, por outro, conferir um regime diferenciado às microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, antes da discussão propriamente dita do assunto no âmbito de seu próprio processo de regulamentação não se mostra eficiente, considerando que o agente de tratamento não é o principal elemento nesta análise, mas, sim, o risco envolvido para o titular de dados³⁴.

Sendo assim, a partir de todo o exposto, recomendamos a supressão do art. 11 disposto na minuta sob análise, tendo em vista que deve-se levar em consideração o grau de risco aos titulares de dados como elemento central para a elaboração do Relatório de Impacto à Proteção de Dados, não havendo qualquer relação com o porte do agente de tratamento. Ademais, o fato de o RIPD ainda não ter sido regulamentado pela Autoridade Nacional de Proteção de Dados, indica que, a princípio, a flexibilização poderia transformar um instrumento tão importante quanto o relatório de impacto em, tão somente, uma ferramenta para demonstrar a adequação à LGPD e mitigar os riscos regulatórios.

Recomendação

Supressão total do art. 11.

Contudo, caso a recomendação não seja aceita e persista a proposta de flexibilização do Relatório de Impacto à Proteção de Dados, é necessário que um conteúdo mínimo seja estabelecido para a condução adequada do referido instrumento, levando em consideração a menor capacidade de estruturação apresentadas pelos agentes de tratamento de pequeno porte, o que reflete uma dificuldade de se apresentar um RIPD completo e detalhado³⁵.

Desse modo, partindo da leitura do art. 5, XVII da LGPD, e partindo da compreensão sobre a função, exercida pelo RIPD, de auxiliar na garantia dos direitos fundamentais e liberdades civis do titular de dados, entendemos que o conteúdo mínimo para a realização simplificada deste processo deve conter a (i) descrição das atividades de tratamento e dos tipos e categorias de dados utilizados e (ii) estabelecimento de medidas de mitigação de riscos existentes e de prevenção de riscos futuros.

34 Ibid p. 43.

35 Ibid p. 51.

Recomendação alternativa

Art. 11. Os agentes de tratamento de pequeno porte podem apresentar o relatório de impacto à proteção de dados pessoais de forma simplificada quando for exigido.

Devendo este relatório conter, minimamente:

I- Descrição das atividades de tratamento de dados pessoais;

II- Descrição dos tipos e categorias de dados utilizados no processo de tratamento;

III- Estabelecimento de medidas, salvaguardas e mecanismos de mitigação de risco.

4. Segurança da Informação

Nesta seção será analisado o disposto nas Seções “IV - Das Comunicações dos Incidentes de Segurança” e “VI - Da Segurança e Boas Práticas”, com destaque à política de segurança da informação simplificada para agentes de pequeno porte.

4.1. Comunicação de incidente de segurança

O art. 12 da minuta proposta indica que a comunicação de incidente de segurança sujeita-se a dispensa, flexibilização ou procedimento simplificado. No dispositivo, chama a atenção a possibilidade de dispensa da comunicação. Quanto ao ponto, ressalta-se que o dever de notificação tem uma natureza dialógica com duas perspectivas, tanto para o titular dos dados pessoais quanto para a ANPD, e que é deflagrado pelo risco e/ou dano ocasionado aos titulares. Por certo, nem todo incidente de segurança deflagra o dever de notificação à ANPD ou aos titulares de dados. Contudo, o elemento que deflagra esse dever é o **risco** ocasionado por esse incidente, nos termos do art. 48, caput da LGPD³⁶.

Assim, o porte do agente de tratamento não deve ser um elemento a se considerar para a dispensa ou flexibilização dessa obrigação. Nada impede, contudo, que procedimentos simplificados e facilitados sejam oferecidos a agentes de pequeno porte. Calibrar e flexibilizar o procedimento para essa comunicação não se confunde, em hipótese alguma, com uma flexibilização ou dispensa desse dever de comunicar.

³⁶ Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Ainda, ressalta-se que um incidente de segurança sempre deflagra um dever: ainda que não o de notificação, no mínimo a adoção de medidas eficazes e o registro do incidente considerado irrelevante, bem como o juízo de valor para considerá-lo irrelevante. Esse elemento reforça a importância do que foi argumentado no tópico 2 a respeito da obrigação de registro das atividades de tratamento.

4.2. Política de segurança simplificada

Além disso, o art. 15 da minuta proposta prevê a possibilidade de agentes de pequeno porte adotarem uma política de segurança simplificada. Embora uma política simplificada possa ser mais adequada para atender a realidade dos agentes de pequeno porte, é importante que a ANPD observe a legislação complementar, de forma a não criar novos conflitos e antinomias.

Nesse sentido, ressalta-se que o Marco Civil da Internet e seu Decreto Regulamentador (Decreto nº 8.771, de 11 de maio de 2016) em suas respectivas seções de padrões de segurança e boas práticas (Capítulo III, Seção II de ambos os normativos), determinam diretrizes e padrões mínimos de segurança que devem ser seguidos por provedores de conexão e aplicação. Embora a LGPD possua um escopo mais amplo do que o Marco Civil da Internet, se aplicando também para dados tratados fora do ambiente da internet, é fundamental manter uma harmonia entre esses dois marcos normativos, visto que muitos agentes de pequeno porte podem atuar como provedores de aplicação.

Portanto, recomenda-se que a ANPD estabeleça como critérios mínimos da política de segurança simplificada o disposto no art. 13 do Decreto nº 8.771:

Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Recomendação

Art. 12. A ANPD poderá dispor sobre **procedimento simplificado ou facilitado para a** comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da resolução específica.

Art. 15. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§1º A política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte, bem como a sensibilidade e a criticidade dos dados tratados diante dos direitos e liberdades do titular.

§2º A política simplificada de segurança da informação deve contar com o estabelecimento de controle de acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso; previsão de mecanismos de autenticação; e gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes, conforme disposto [no art. 13 do Decreto nº 8.771, de 11 de maio de 2016](#).

§3º A ANPD considerará a existência das políticas simplificadas de segurança da informação para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.

5. Indicação de Encarregado

Originalmente, a figura do encarregado, conceituada no art. 5º, inciso VIII, da LGPD, seria obrigatória para todas as organizações que realizam tratamento de dados pessoais no âmbito de aplicação da LGPD, independentemente de seu tamanho ou de serem públicas ou privadas. Porém,

com a minuta de resolução da ANPD sobre agentes de tratamento de pequeno porte, em conjunto com o art. 41, § 3º da LGPD, a obrigação de nomeação seria dispensada de forma integral para esses agentes.

Em um cenário ideal, com o intuito de assegurar a correta proteção de direitos e liberdades fundamentais dos titulares de dados, a obrigatoriedade de indicação do encarregado deveria ocorrer para todas as instituições que possuam modelo de negócio baseado no tratamento de dados pessoais, sejam eles triviais ou sensíveis, ou cujas atividades sejam consideradas de alto risco para os direitos e liberdades fundamentais.

Isso porque o tamanho ou a natureza da organização, por si só, não definem a complexidade e a criticidade de duas atividades para a proteção de dados pessoais. Desta forma, a obrigatoriedade de indicação do Encarregado deve ser direcionada também para agentes de tratamento de pequeno porte, mas cujas atividades representam um elevado risco aos direitos e liberdades fundamentais dos titulares de dados.

Por isso, a minuta proposta pela Autoridade acerta ao dispensar da obrigatoriedade de nomeação do encarregado apenas os agentes de tratamento de pequeno porte cobertos pela referida resolução, pois traz expressamente a exceção de aplicação de suas regras para aqueles agentes de tratamento de pequeno porte que realizem tratamento de alto risco (aqui, já considerando a melhor interpretação de utilização do elemento de “larga escala” como um dos critérios de análise do alto risco).

Apesar da dispensa de obrigatoriedade de nomeação de encarregado, considera-se essa indicação como uma boa prática por parte dos agentes de tratamento, garantindo maior proteção aos direitos e liberdades fundamentais dos titulares de dados, o que deve ser expressamente estipulado pela Autoridade Nacional de Proteção de Dados na futura resolução.

Considerando a abordagem de regulação responsiva da ANPD, que leva em consideração incentivos positivos e negativos do comportamento do agente regulado e os níveis de gravidade de violações da LGPD, a nomeação de encarregado pelo agente de pequeno porte dispensado de tal necessidade pode ser uma boa prática potencialmente considerada pela Autoridade em eventuais procedimentos sancionatórios, o que funcionaria como incentivo à implementação de tais práticas pelo agente de tratamento de dados de pequeno porte, mesmo diante da ausência de obrigatoriedade.

É sabido, porém, que a indicação de um encarregado, seja ele representado por uma pessoa jurídica ou física, externa ou interna da organização, pode ser um encargo financeiro relevante para os agentes de tratamento de pequeno porte³⁷. Com o intuito de superar ou reduzir tal dificuldade, a ANPD

37 Centre for Information Policy Leadership (CIPL); Centro de Direito, Internet e Sociedade (CEDIS-IDP). Prioridades das Organiza-

poderia prever também a possibilidade de nomeação de um mesmo encarregado por um conjunto de associações, fundações microempresas, pequenos empresários e startups, quando reunidos em uma associação, nos moldes do que foi sugerido no art. 9º da minuta de Resolução aqui em análise.

Parece ser essa a abordagem adotada no cenário internacional no âmbito do Regulamento de Proteção de Dados Pessoais da União Europeia (GDPR), especificamente no art. 37 (4). No contexto europeu, o GDPR expressamente indica as hipóteses em que a nomeação do encarregado é necessária, trazendo estímulos para que a nomeação ocorra mesmo em casos de dispensa, ao prever a possibilidade de um único encarregado para associações de empresas ou de entidades que representam os agentes de tratamento em conjunto.

Tal possibilidade é expressamente mencionada pela Autoridade Nacional de Proteção de Dados no Relatório de Análise de Impacto Regulatório realizado para a construção do modelo regulatório para aplicação da LGPD a microempresas e empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais. De acordo com a própria ANPD, as entidades de representação podem funcionar como apoio aos agentes de tratamento de pequeno porte em questões referentes aos direitos dos titulares³⁸, o que poderia ser igualmente implementado no caso da nomeação de encarregado, em conjunto, por essas entidades.

Recomendação

Ainda que a Autoridade Nacional de Proteção de Dados decida pela dispensa da indicação de um encarregado para agentes de pequeno porte, é essencial que exista um incentivo e um reconhecimento para que esses atores indiquem seus encarregados, o que pode ser feito em conjunto por entidades de representação ou associações de classe de agentes de pequeno porte, mesmo em casos de dispensa. Tal comportamento deve ser interpretado como uma boa prática de governança de dados, que pode ser considerado positivamente em eventuais procedimentos sancionatórios no âmbito da regulação responsiva.

Assim, há desenvolvimento de estímulos em prol da proteção dos dados pessoais dos titulares, assim como de seus direitos e liberdades fundamentais, além de facilitar a criação e consolidação de uma cultura de proteção de dados dentro das organizações.

ções Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD). 2020. p. 8.

38 Autoridade Nacional de Proteção de Dados (ANPD). Relatório de Análise de Impacto Regulatório realizado para a construção do modelo regulatório para aplicação da LGPD a microempresas e empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais. Disponível em: <<https://www.gov.br/participamaisbrasil/blob/baixar/7871>>.

Seção V

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 13. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.

§1º A indicação de encarregado por agentes de pequeno porte será considerada para os fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.

§2º Fica facultado aos agentes de tratamento de pequeno porte nomearem o encarregado por meio de entidades de representação da atividade organizacional, por pessoas jurídicas ou por pessoas naturais.

Parágrafo único §3º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados.

6. Prazos diferenciados

O artigo 16 da minuta proposta prevê a concessão de prazo em dobro para agentes de pequeno porte em algumas hipóteses, sendo uma delas a de comunicação de incidente de segurança, em seu inciso II. Nesse sentido, o dispositivo destacado aborda dois tipos de notificação: uma à Autoridade, outra aos titulares. Ainda que ambos se aproximem por buscarem sempre a limitação dos danos ocasionados pelo incidente, há diferenças notáveis quanto aos objetivos de cada comunicação e, portanto, em suas respectivas abordagens.

Em relação ao prazo de notificação à ANPD, como regra, os critérios de celeridade e tempo razoável para identificação do nível de risco e dano, visto que a notificação à Autoridade busca, dentre outros elementos, oferecer-lhe subsídios para uma investigação e mitigação de danos.

Por sua vez, a comunicação ao titular tem como objetivo alertar sobre os riscos ao que este pode estar sujeito em razão do incidente. Em outras palavras, essa notificação específica para o titular busca dar ciência do ocorrido, de forma a fornecer informações específicas sobre as etapas que devem seguir para proteger seus dados e, caso necessário, buscar mais informações.

Além de cumprirem objetivos diferentes, as notificações também se dão de forma distinta, quando feita a um titular de dados e quando feita à Autoridade Nacional de Proteção de Dados. Ao

contrário da comunicação aos titulares, não existem grandes empecilhos para identificar o canal de recebimento de comunicação e os meios pelo qual essa comunicação deva ser realizada. É possível ainda que, em regulamentação específica, a ANPD disponha sobre uma comunicação faseada de incidentes de segurança. Ou seja, caso o agente de tratamento tenha dificuldades de coletar todas as informações para uma comunicação completa para a Autoridade, ele poderia primeiro fazer uma comunicação simplificada e, em segundo momento, complementá-la com mais informações. Nesse sentido, a concessão de prazo em dobro para comunicar um incidente à ANPD mostra-se desproporcional, visto que esta poderia se dar de forma simplificada.

Por outro lado, a comunicação aos titulares afetados por um incidente de segurança pode de fato apresentar dificuldades para agentes de pequeno porte. Sendo assim, há sentido em se conceder um prazo adicional, desde que alguma comunicação já tenha sido feita para a ANPD. Essa comunicação imediata à ANPD é fundamental até mesmo para que a Autoridade possa orientar o agente de pequeno porte se o incidente em questão se enquadra na hipótese de prazo em dobro ou não, visto que a própria minuta de resolução já reconhece que em casos em que houver risco à integridade dos titulares ou à segurança nacional essa flexibilização não se aplicaria.

Por fim, a aferição de risco à integridade dos titulares deve levar em conta não só a integridade física, mas também moral. Dito isso, poderia-se considerar como critérios considerados para essa aferição o tipo de incidente; a natureza, sensibilidade, e volume de dados pessoais; os tipos de titulares atingidos, suas relações com os agentes e se há menores de idade envolvidos; e a severidade de consequências para os indivíduos, conforme disposto no art. 48, §1o, IV, da LGPD.

Recomendação

Art. 16. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:

II - na comunicação **ao titular** da ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos titulares, nos termos da resolução específica, exceto quando houver potencial comprometimento à integridade **física ou moral** dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada resolução;

7. Direitos dos titulares

A minuta da norma de aplicação da LGPD para microempresas e empresas de pequeno porte prevê, ainda, dispensas e flexibilizações para obrigações dos agentes de tratamento de pequeno porte relacionadas aos direitos dos titulares. Nesse sentido, será destacado na nossa análise o disposto no art. 6º, §1º, art. 6º, §2º, art. 7.

7.1. Direito de solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD

Primeiramente, a flexibilização proposta no art. 6º §2º se mostra uma escolha arriscada e que pode ter consequências negativas não previstas pela Autoridade Nacional de Proteção de Dados. Conforme descrito na Análise de Impacto Regulatório disponibilizada pela ANPD, os custos e a complexidade envolvida em processos de anonimização são muito elevados, criando uma barreira para agentes de pequeno porte.

Considera-se acertada essa preocupação levantada pela Autoridade. Contudo, a maneira com que essa flexibilização está prevista pode gerar um outro tipo de consequência indesejada. Ao dar a opção para esses agentes anonimizar dados tratados em desconformidade, ao invés de eliminá-los ou bloqueá-los, pode-se criar um incentivo que irá banalizar o conceito de anonimização. Agentes podem alegar que, quando solicitados, irão anonimizar dados ao invés de excluí-los, quando, na verdade, podem estar empregando técnicas frágeis de anonimização, o que leva, em última análise, a uma desproteção dos titulares de dados ainda maior, caminhando também em direção contrária ao princípio da necessidade.

Portanto, uma solução para esse impasse seria optar que os agentes de pequeno porte possam escolher entre eliminar ou bloquear dados desnecessários, excessivos ou tratados em desconformidade, ainda que o titular solicite a anonimização.

7.2. Direito de confirmação de existência ou de acesso a dados pessoais por meio de declaração clara e completa

Além disso, o art. 7º da minuta dispensa os agentes de atenderem a solicitação do titular de obter informações completas sobre as atividades de tratamento de dados que envolvam seus dados pessoais. Essa dispensa total se mostra inadequada e excessiva.

A declaração completa sobre atividades de tratamento realizadas com os dados de um titular é fundamental não só para a materialização do princípio da transparência e da responsabilização e

prestação de contas, mas também para destravar e possibilitar o exercício de todos os direitos previstos pela legislação. Isso porque, sem primeiro saber quais atividades de tratamento são realizadas, quais dados são utilizados e para qual finalidade, não se pode sequer saber quais direitos são passíveis de serem exercidos.

Para que um titular se oponha a uma atividade de tratamento (art. 18 §2º da LGPD), por exemplo, é necessário que ele saiba que essa atividade está sendo realizada e para qual finalidade. Além disso, alguns direitos dos titulares estão condicionados à base legal que fundamenta a atividade, como é o caso do direito de cópia eletrônica integral, previsto pelo art. 19 §3º da LGPD, aplicável quando o tratamento tiver origem no consentimento do titular ou em contrato.

Caso essa declaração completa seja muito custosa para os agentes de pequeno porte, recomenda-se que a ANPD estabeleça formas facilitadas, templates, manuais específicos ou até mesmo concessão de prazo ampliado para que esses agentes possam cumprir com requisitos mínimos. Contudo, a completa dispensa dessa obrigação amplia a vulnerabilidade e a desproteção dos titulares de dados, dificultando ainda mais o exercício dos demais direitos. Isentar os agentes de tratamento de dados dessa obrigação abre uma grave lacuna para que os agentes possam tratar dados em desconformidade com a lei e os titulares não tenham acesso aos meios necessários para contestar esse tratamento.

7.3. Direito à portabilidade

Por fim, em relação a dispensa de conferir portabilidade dos dados dos titulares, previsto pelo art. 6º, §1º da norma proposta, há de se considerar que, além de ampliar a vulnerabilidade e reduzir as garantias dos titulares de dados, conforme já argumentado acima, há também um elemento concorrencial atrelado a esse direito. Dispensar agentes de pequeno porte desse direito pode fazer com que novos atores tenham mais dificuldade de entrar em mercados. Portanto, acreditamos que deve haver uma lógica precaucionária ainda mais forte na dispensa dessa obrigação.

De todo modo, ainda que a opção pela dispensa total seja mantida pela Autoridade, seria importante e recomendável que ao menos houvesse uma comprovação, por parte do agente de tratamento, da dificuldade de realizar essa portabilidade. Isso porque alguns setores, como o setor financeiro, possuem tecnologias e padrões de interoperabilidade em que essa portabilidade tem um custo reduzido, o que não seria condizente com a dispensa, enquanto outros setores podem apresentar custos mais altos, que tornariam a dispensa justificável.

CAPÍTULO II
DAS OBRIGAÇÕES DO AGENTE DE TRATAMENTO DE PEQUENO PORTE

Seção I
Das obrigações relacionadas aos direitos do titular

Art. 6º Os agentes de tratamento de pequeno porte podem atender às requisições dos titulares de dados pessoais, descritas no art. 18 da LGPD, por meio eletrônico ou impresso.

§1º Os agentes de tratamento de pequeno porte estão dispensados de conferir portabilidade dos dados do titular a outro fornecedor de serviço ou produto, nos termos do inciso V do art. 18 da LGPD, **desde que comprovada a dificuldade técnica para operacionalização da portabilidade.**

§2º É facultado ao agente de tratamento de pequeno porte, quando solicitado pelo titular de dados, optar entre **bloquear ou eliminar** os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, na forma do art. 18, inciso IV, da LGPD, **ainda que o titular solicite a anonimização de seus dados.**

Art. 7º Os agentes de tratamento de pequeno porte **podem fornecer a declaração** clara e completa de que trata o art. 19, inciso II, da LGPD **em modelo simplificado, que será disponibilizado pela ANPD.**

CONCLUSÃO

A partir do argumentado na presente contribuição, apresentamos a tabela abaixo sintetizando todas as recomendações propostas de alteração de texto normativo.

Tabela de recomendações e sugestões de texto

Texto original	Recomendações ou sugestões de texto
<p>Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:</p> <p>I - microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º da Lei Complementar nº 123, de 14 de dezembro de 2006;</p> <p>II - startups: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021;</p> <p>III - pessoas jurídicas sem fins lucrativos: associações, fundações, organizações religiosas e partidos políticos;</p> <p>IV - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento</p>	<p>Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:</p> <p>I - microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º da Lei Complementar nº 123, de 14 de dezembro de 2006;</p> <p>II – startups: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021;</p> <p><i>III - pessoas jurídicas sem fins lucrativos: associações e fundações;</i></p> <p>IV – agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas</p>

<p>de dados pessoais, assumindo obrigações típicas de controlador ou de operador;</p> <p>V - zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.</p> <p>Parágrafo único. Para fins desta resolução, consideram-se, ainda, agentes de tratamento de pequeno porte os que possuem receita bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.</p>	<p>de controlador ou de operador;</p> <p>V – zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.</p> <p>VI - dados de titulares vulneráveis: dados pessoais de titulares em condição de hipervulnerabilidade em relação ao agente de tratamento, como crianças, adolescentes, idosos e pessoas com deficiência.</p> <p>Parágrafo único. Para fins desta resolução, consideram-se, ainda, agentes de tratamento de pequeno porte, os que possuem receita bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.</p>
<p>Art. 3º A dispensa e a flexibilização das obrigações previstas nesta resolução não são aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares, ressalvada a hipótese prevista no art. 13, Parágrafo único.</p> <p>§1º Para fins desta resolução, será considerado tratamento de alto risco para os titulares, entre outras hipóteses, o tratamento que envolva:</p> <p>I - dados sensíveis ou dados de grupos vulneráveis, incluindo crianças e adolescentes e idosos;</p> <p>II - vigilância ou controle de zonas acessíveis ao público;</p> <p>III - uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; ou</p> <p>IV - tratamento automatizado de dados pessoais</p>	<p>Art. 3º A dispensa e a flexibilização das obrigações previstas nesta resolução não são aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 13, Parágrafo único.</p> <p>§1º Para fins desta resolução, será considerado tratamento de alto risco para os titulares, entre outras hipóteses, o tratamento que envolva:</p> <p>I - atividade de tratamento de dados em larga escala</p> <p>II - dados sensíveis ou dados de titulares vulneráveis, incluindo dados de condenações criminais, além de dados de crianças e adolescentes, pessoas com deficiência, idosos e quaisquer outros que se enquadrem na definição do art. 2º, inciso VI;</p> <p>III - vigilância ou controle de zonas acessíveis ao público;</p> <p>IV - uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares,</p>

que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 2º O tratamento de dados será caracterizado como de larga escala quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

§ 3º Para fins deste artigo não será considerado tratamento de larga escala o tratamento de dados de funcionários ou para fins exclusivos de gestão administrativa do agente de tratamento de pequeno porte.

§ 4º A ANPD disponibilizará guias e orientações que auxiliem os agentes de tratamento de pequeno porte a avaliar se realizam tratamento com alto risco e em larga escala.

tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; ou

V - tratamento automatizado de dados pessoais que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 2º O tratamento de dados será caracterizado como de larga escala quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

§ 3º Para fins deste artigo não será considerado tratamento de larga escala o tratamento de dados de funcionários ou para fins exclusivos de gestão administrativa do agente de tratamento de pequeno porte.

§ 4º A ANPD disponibilizará guias e orientações que auxiliem os agentes de tratamento de pequeno porte a avaliar se realizam tratamento com **alto risco**.

§ 5º A dispensa e a flexibilização das obrigações previstas nesta resolução também não se aplicam a agentes de tratamento de pequeno porte que façam parte de conglomerados ou grupos econômicos formados por agentes de tratamento de grande porte que realizem tratamento de alto risco para os titulares.

Art. 6º Os agentes de tratamento de pequeno porte podem atender às requisições dos titulares de dados pessoais, descritas no art. 18 da LGPD, por meio eletrônico ou impresso.

§1º Os agentes de tratamento de pequeno porte

Art. 6º Os agentes de tratamento de pequeno porte podem atender às requisições dos titulares de dados pessoais, descritas no art. 18 da LGPD, por meio eletrônico ou impresso.

§1º Os agentes de tratamento de pequeno porte

<p>estão dispensados de conferir portabilidade dos dados do titular a outro fornecedor de serviço ou produto, nos termos do inciso V do art. 18 da LGPD.</p> <p>§2º É facultado ao agente de tratamento de pequeno porte, quando solicitado pelo titular de dados, optar entre anonimizar, bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, na forma do art. 18, inciso IV, da LGPD.</p>	<p>estão dispensados de conferir portabilidade dos dados do titular a outro fornecedor de serviço ou produto, nos termos do inciso V do art. 18 da LGPD, desde que comprovada a dificuldade técnica para operacionalização da portabilidade.</p> <p>§2º É facultado ao agente de tratamento de pequeno porte, quando solicitado pelo titular de dados, optar entre bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, na forma do art. 18, inciso IV, da LGPD, ainda que o titular solicite a anonimização de seus dados.</p>
<p>Art. 7º Os agentes de tratamento de pequeno porte ficam dispensados de fornecer a declaração clara e completa de que trata o art. 19, inciso II, da LGPD.</p>	<p>Art. 7º Os agentes de tratamento de pequeno porte podem fornecer a declaração clara e completa de que trata o art. 19, inciso II, da LGPD em modelo simplificado, que será disponibilizado pela ANPD.</p>
<p>Art. 10. Os agentes de tratamento de pequeno porte ficam dispensados da obrigação de manutenção de registros das operações de tratamento de dados pessoais constante do art. 37 da LGPD.</p> <p>Parágrafo único. A ANPD fornecerá modelos para o registro voluntário e simplificado das atividades de tratamento por agentes de tratamento de pequeno porte, e considerará a existência de tais registros para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.</p>	<p>Art. 10. Os agentes de tratamento de pequeno porte deverão elaborar e manter os registros das operações de tratamento de dados pessoais constantes do art. 37 da LGPD.</p> <p>Parágrafo único. A ANPD fornecerá modelos para o registro simplificado das atividades de tratamento por agentes de tratamento de pequeno porte.</p>
<p>Art. 11. Os agentes de tratamento de pequeno porte podem apresentar o relatório de impacto à proteção de dados pessoais de forma simplificada quando for exigido, nos termos da resolução específica.</p>	<p>Recomendação principal: Supressão do art. 11</p> <p>Recomendação subsidiária: Art. 11. Os agentes de tratamento de pequeno porte podem apresentar o relatório de impacto à proteção de dados pessoais de forma simplificada quando for exigido. Devendo este relatório conter, minimamente:</p> <p>I- Descrição das atividades de tratamento de dados</p>

	<p>personais</p> <p>II- Descrição dos tipos e categorias de dados utilizados no processo de tratamento</p> <p>III- Estabelecimento de medidas, salvaguardas e mecanismos de mitigação de risco</p>
<p>Art. 12. A ANPD poderá dispor sobre dispensa, flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da resolução específica.</p>	<p>Art. 12. A ANPD poderá dispor sobre procedimento simplificado ou facilitado para a comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da resolução específica.</p>
<p>Art. 13. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.</p> <p>Parágrafo único. O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados.</p>	<p>Art. 13. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.</p> <p>§1º A indicação de encarregado por agentes de pequeno porte será considerada para os fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.</p> <p>§2º Fica facultado aos agentes de tratamento de pequeno porte nomearem o encarregado por meio de entidades de representação da atividade organizacional, por pessoas jurídicas ou por pessoas naturais.</p> <p>Parágrafo único §3º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados.</p>
<p>Art. 14. Os agentes de tratamento de pequeno porte devem adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.</p>	

<p>Parágrafo único. A ANPD disponibilizará guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.</p>	
<p>Art. 15. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.</p> <p>§1º A política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte, bem como a sensibilidade e a criticidade dos dados tratados diante dos direitos e liberdades do titular.</p> <p>§2º A ANPD considerará a existência das políticas simplificadas de segurança da informação para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.</p>	<p>Art. 15. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.</p> <p>§1º A política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte, bem como a sensibilidade e a criticidade dos dados tratados diante dos direitos e liberdades do titular.</p> <p>§2º A política simplificada de segurança da informação deve contar com o estabelecimento de controle de acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso; previsão de mecanismos de autenticação; e gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes, conforme disposto no art. 13 do Decreto nº 8.771, de 11 de maio de 2016.</p> <p>§3º A ANPD considerará a existência das políticas simplificadas de segurança da informação para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.</p>
<p>Art. 16. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:</p> <p>I - no atendimento das solicitações dos titulares</p>	<p>Art. 16. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:</p> <p>II - na comunicação ao titular da ocorrência de inci-</p>

referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, parágrafos 3º e 5º, nos termos da resolução específica;

II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da resolução específica, exceto quando houver potencial comprometimento à integridade dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada resolução;

III - 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. Parágrafo único. Os prazos não especificados nesta resolução para agentes de tratamento de pequeno porte serão determinados por resoluções específicas.

dente de segurança, que possa acarretar risco ou dano relevante aos titulares, nos termos da resolução específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada resolução;