Item 42

Art. 5º Para fins deste Regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar **risco ou dano relevante** aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e envolver pelo menos um dos seguintes critérios:

Contribuição: Sugerimos a inclusão do Inciso XVIII no art.3º (Definições) da proposta desta Consulta pública, trazendo um critério mais claro e objetivo para definir as expressões "**Risco" e "Dano Relevante",** de modo que os agentes de tratamento (Controlador e Operador) tenham segurança operacional e jurídicas adequadas para a efetiva comunicação dos incidentes de segurança aos titulares e à autoridade.

Justificativa: Apesar do caráter abstrato da lei para garantir sua abrangência e atingimento de finalidade, se faz necessária uma definição do que deve ser classificado como risco ou dano relevante e que leve em conta não a natureza de dano e risco, mas sim sua efetiva gravidade. Riscos, por definição, são identificáveis e mensuráveis, e, portanto, sua definição em razão da gravidade se mostra razoável no caso prático de incidentes de segurança, pois somente assim não haverá banalização e descredito deste instrumento de comunicação de incidente de segurança. É fundamental que a ANPD estabeleça critérios mais objetivos e orientações claras que possibilitem a avaliação concreta do incidente e aferição adequada de potenciais riscos e danos.

Algumas referências europeias estabelecem fatores mais claros a ser observados nesse tipo de avaliação, como o *Guidelines 9/2022 on personal data breach notification under GDPR*, emitida *pelo European Data Protection Board*. Este documento apresenta aborda aspectos, como:

1. Tipo de violação (por exemplo, violação de confidencialidade);
2. Natureza, sensibilidade e volume dos dados pessoais;
3. Facilidade de identificação de indivíduos, seja de maneira direta ou indireta;
4. Gravidade das consequências para os indivíduos, a depender da natureza dos dados pessoais envolvidos em uma violação e dano potencial a indivíduos.
5. Características especiais dos indivíduos, por exemplo, dados relativos a crianças ou outros indivíduos vulneráveis;
6. Características especiais do controlador de dados, levando em consideração a natureza, o papel do controlador e as atividades desempenhadas no mercado
7. Número de indivíduos afetados

Nesse sentido, o próprio formulário de Comunicação de Incidentes publicado pela ANPD em dezembro de 2022 exige que sejam informados à autoridade quesitos que se assemelham aos critérios supracitados:

1. De que forma o incidente afetou os dados pessoais
2. Quais os tipos e descrição de dados pessoais sensíveis violados
3. Quais os demais tipos e descrição de dados pessoais violados
4. A elaboração ou não de um Relatório de Impacto

5. Qual a quantidade aproximada de titulares afetados
6. Quais as categorias de titulares afetados pelo incidente
7. Quais as prováveis consequências do incidente para os titulares
8. Quais as prováveis consequências e impactos do incidente para titulares

Nota-se, assim, que o espectro da avaliação da ANPD em relação a um incidente de dados pessoais já comporta critérios mais objetivos, tendo em vista que as respectivas informações são assim exigidas no atual processo de notificação vigente. É necessário que tal se reflita em regulamento adequado, de forma que haja clareza para o agente de tratamento de sua vinculação