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:*
III - dados financeiros;

1

É importante mencionar que a LGPD não define dados financeiros, tampouco criou distinções entre categorias de dados pessoais, tal qual a classificação proposta pela minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. Além disso, a definição de "dado financeiro" proposta não se encontra alinhada com as legislações bancárias e financeiras, incluindo a Lei de Sigilo Bancário (Lei Complementar nº 105). No limite, na definição atualmente proposta, qualquer dado cadastral sobre transações financeiras se enquadraria como "dado financeiro", o que não é compatível com o entendimento atualmente consolidado sobre o tema. Sendo assim, sugere-se a exclusão dessa categoria de dados, bem como sua qualificação como critério para avaliar se um incidente de segurança pode acarretar risco ou dano relevante aos titulares.

Art. 5º
§ 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam:
I - impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou

O artigo 5º, § 1º da minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais estabelece que um incidente de segurança com dados pessoais que cause o impedimento ou a limitação da utilização de um serviço teria o potencial de afetar significativamente os interesses e os direitos fundamentais dos titulares. Esta proposição é desproporcional. Em primeiro lugar, a paralisação de um serviço, de forma abstrata e genérica, não significa necessariamente uma violação aos interesses e direitos fundamentais dos titulares. Isso porque existem diversos serviços que, ainda quando impedidos ou limitados, não violariam as liberdades e as garantias dos titulares. Basta imaginar as diferenças entre a paralisação de serviços essenciais, conforme elencados no artigo 10 da Lei Federal n.º 7.783/1989, em face da de serviços não-essenciais: não é proporcional que a Autoridade Nacional de Proteção de Dados iguale ambos os casos.

Ainda que eventuais prejuízos ao fornecimento de serviços tenham impactos consideráveis aos agentes de tratamento de dados pessoais, o mesmo não ocorre necessariamente aos titulares consumidores, motivo pelo qual não faz sentido a abrangência estipulada pelo artigo 5º, § 1º do Regulamento. Essa previsão, da maneira em que se encontra, não parece adequada para resguardar o titular dos dados pessoais. Uma restrição realmente fundamentada poderia, por exemplo, pautar-se em um impedimento ou em uma limitação de utilização de um serviço que efetivamente seja capaz de violar os direitos e as garantias fundamentais da pessoa humana. A espécie do serviço é um vetor importante que deve ser levado em conta pela ANPD.

> ***Art. 5º***
> *§ 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam:*
> *II - ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade.*

A Autoridade Nacional de Proteção de Dados tem suas competências delimitadas especificamente pelo artigo 55-J, da Lei Geral de Proteção de Dados Pessoais. Assim, não é possível vislumbrar qualquer possibilidade de a Autoridade determinar, por si só, o que configura uma hipótese de dano material ou moral ao titular dos dados pessoais. Além disso, o estabelecimento do nexo causal em eventuais incidentes de segurança com dados pessoais é questão amplamente controvertida na doutrina especializada. Demonstra-se bastante tortuoso identificar o liame lógico entre eventual incidente de segurança e o dano suportado pelo titular dos dados pessoais. E a bem da verdade, sem essa comprovação, não há que se falar em responsabilização e em existência de dano material ou moral.

Com isso, deve-se atentar que o Poder Judiciário é a esfera competente para identificar a existência de danos em incidentes de segurança com dados pessoais. Não cabe em esfera administrativa, portanto, presumir hipóteses exemplificativas de ocorrência de danos morais aos titulares: ao contrário, eventuais violações devem ser comprovadas em sede judicial, para fins de atestar se determinado evento adverso confirmado efetivamente se relaciona com circunstâncias que possam configurar dano ao titular dos dados pessoais.

De outro lado, o texto deve explicitar que a discriminação a ser combatida é aquela que se revele *ilícita* ou *abusiva* (cf. art. 6º, IX, da LGPD). Ao não trazer distinções quanto à licitude e à abusividade da discriminação, grande parte das análises de crédito realizadas pelos bureaus, acaso mantido o projeto tal como está, pode ser tida como discriminatória e, portanto, proibidas - embora sejam lícitas, benéficas e imprescindíveis à sociedade, sendo, inclusive, expressamente estabelecida em nosso ordenamento jurídico vigente como indispensável à efetiva prevenção e tratamento do fenômeno do superendividamento.

Art. 5º
§ 2º Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.

A definição de “larga escala” se mostra muito abrangente. Faz-se necessário uma definição objetiva de larga escala. Consideramos ainda importante ser levado em conta a proporção de dados afetados pelo incidente *versus* a quantidade de dados tratados pelo Controlador.

***Art. 6º** A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:*

O *caput* do artigo 6º da minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais estabelece que a comunicação do incidente de segurança com dados pessoais terá como termo inicial o conhecimento do evento adverso confirmado pelo agente de tratamento. Para tanto, a ANPD deve oferecer critérios objetivos a fim de identificar quando efetivamente se tomaria conhecimento do incidente. A previsão do Regulamento se assemelha com o Considerando 85 e com o artigo 33 do Regulamento Geral sobre Proteção de Dados da União Europeia ("GDPR"). Por essas razões, mostra-se como importante referencial teórico o material "Guidelines on Personal data breach notification under Regulation 2016/679" do European Data Protection Board.

No documento, considera-se que o agente de tratamento tomaria conhecimento do incidente de segurança com dados pessoais assim que existisse um grau razoável de certeza de que o evento adverso se concretizou. Todavia, reconhece-se que são as circunstâncias do evento adverso que irão ditar as condições exatas em que o agente de tratamento ficou a par da situação. Isso porque em alguns casos pode ser relativamente evidente a ocorrência do incidente de segurança com dados pessoais; em outros, porém, poderá ser necessário um lapso temporal maior para apurar a ocorrência da violação. Assim, a um potencial incidente de segurança com dados pessoais pode-se seguir um "período de investigação" interno para confirmar ou ter evidências concretas – nesse momento, entende-se que o agente de tratamento ainda não teria tomado conhecimento do evento adverso.

Nessa direção, recomenda-se que a ANPD especifique, com maiores detalhes, o momento no qual o agente de tratamento passa a ter efetivamente “conhecimento” do incidente, sendo certo que esse momento deve levar em consideração elementos razoáveis de concretização do incidente, admitindo, se for o caso, período anterior de investigação interna.

A sugestão é que o início da contagem do prazo deve se dar a partir da conclusão, do controlador, de que o incidente envolve dados pessoais e pode acarretar risco ou dano relevante aos titulares. Essa comunicação deverá conter as informações preliminares até então já verificadas pelo Controlador, sendo complementadas no prazo de 20 dias úteis, estabelecidas pelo parágrafo 1 do art. 6°.

> ***Art. 6º*** *A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:*
> *II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;*

A LGPD não impõe qualquer obrigação específica a agentes de tratamento de dados pessoais em relação a titulares idosos. A ANPD, conforme estabelecido pelo artigo 55-J, XIX, da LGPD, somente deveria garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento. Com efeito, não há previsão de tratamento especial à população idosa na LGPD na mesma proporção com que se verifica a proteção conferida a crianças e adolescentes. Tratando-se de proteção especial que não se justifica em face da LGPD e da realidade brasileira, recomenda-se a supressão dessa previsão ou a sua redução para pessoas idosas com mais de 80 (oitenta) anos, as quais possuem prioridade consoante o artigo 3º, § 2º, do Estatuto do Idoso.

> ***Art. 6º*** *A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:*
> XI - a declaração de que foi realizada a comunicação aos titulares, nos termos do art. 10 deste Regulamento.

Recomenda-se que este inciso seja suprimido uma vez que a comunicação à ANPD deverá ser realizada anteriormente ao envio do comunicado aos titulares de dados, salientando que, da forma como redigida, pressupõe-se que a comunicação aos titulares deve se dar antes, ou seja, em prazo menor que 3 dias, o que se mostra totalmente inexequível.

> ***Art. 6º*** *A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:*
> *XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.*

A ANPD estabelece como requisito para a comunicação de incidente de segurança com dados pessoais à Autoridade a informação do total de titulares cujas informações sejam tratadas pelo agente de tratamento e na atividade afetada pelo evento adverso confirmado. Essa previsão não parece guardar relação com o incidente de segurança e pode representar um ônus desnecessário ao agente de tratamento. Nesse sentido, o artigo 33 do Regulamento Geral sobre Proteção de Dados da União Europeia ("GDPR") prevê como requisito para a comunicação tão somente a indicação do número aproximado de titulares afetados pelo incidente de segurança com dados pessoais. Ante ao exposto, considerando a desnecessidade de conhecimento das informações dispostas no artigo 6º, XIII da minuta do Regulamento, recomenda-se a exclusão do dispositivo.

> ***Art. 7º*** *Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.*

O exemplo de sigilo previsto no artigo 7º da minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais não pode ser a única exceção para a hipótese de restrição de acesso às informações sobre o evento adverso confirmado. É importante observar que o artigo 55-J, II, da LGPD estabelece como competência da ANPD zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos da disciplina da proteção de dados pessoais. Além disso, o artigo 55-J, § 5º, da LGPD prevê que no exercício das competências da ANPD, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei.

Por essas razões, a especificação de sigilo sobre a informação acerca da atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial não pode ser tida como a única espécie possível de sigilo a ser solicitado à ANPD. Logo, seria recomendável suprimir a previsão disposta, a fim de permitir uma proteção mais genérica e eficaz aos agentes de tratamento, da seguinte maneira: "*Art. 7º Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido.*"

> ***Art.*** *9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, no prazo de três dias úteis contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações (...)*

Entendemos como ponto de melhoria o início da contagem do prazo. Isso porque uma comunicação ao titular, de forma precoce, pode gerar mais problemas do que soluções, pode causar alarde desnecessário. O ideal seria que a comunicação ao titular acontecesse após a apreciação do incidente pela ANPD, em que ficaria deliberado: gravidade do incidente, medidas técnicas cabíveis para mitigação dos riscos, entre outros, aumentando também o prazo, para no mínimo 10 dias úteis, dada a complexidade envolvida em tal comunicação. Ainda que não fixado o início da contagem do prazo tal como sugerido, o fato é que o prazo de 3 (três) dias fixado se mostra inexequível.

> ***Art. 9º***
> *§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, seis meses.*

O prazo mínimo de seis meses para a comunicação indireta aos titulares dos dados pessoais afetados por um determinado incidente de segurança com dados pessoais mostra-se desproporcional e muitas vezes pode não ser compatível com as repercussões do evento adverso confirmado. Assim, a definição de uma regra geral pela ANPD deveria considerar as diferentes circunstâncias da ocorrência – a título de exemplo, um incidente de segurança com dados pessoais que afetasse milhões de titulares potencialmente precisaria permanecer publicamente acessível por mais tempo do que uma violação que atingisse apenas uma dezena de pessoas.

Todavia, uma análise caso a caso é essencial para identificar outros parâmetros igualmente relevantes, como a natureza dos dados pessoais envolvidos, ou os riscos relacionados ao incidente e possíveis impactos aos titulares. Dessa forma, recomenda-se que a Autoridade revise essa obrigação, de modo a garantir um período de publicização menos desarrazoado, como o de 2 (dois) meses, reservando à Autoridade a possibilidade de solicitar a manutenção do comunicado por um período maior de tempo.

Cumpre destacar que o balanceamento do período mínimo de seis meses para a publicização da comunicação também é relevante para fins de combater práticas predatórias da advocacia. O excesso de judicialização não é a solução para um país que efetivamente busque desenvolver uma cultura efetiva de privacidade e de proteção de dados pessoais. A bem da verdade, a atuação desta Autoridade tem se pautado justamente pelos objetivos de educar e de incentivar a conformidade dos agentes de tratamento à LGPD e às melhores práticas de segurança da informação. Assim, a publicização não pode ser temporalmente desproporcional de modo a encorajar a má-fé da litigância predatória, mas deve voltar-se justamente aos titulares afetados, conforme preceitua o artigo 48 da LGPD.

***Art. 18**. A ANPD poderá, a qualquer momento, realizar auditorias ou inspeções junto aos agentes de tratamento, ou determinar a sua realização para coletar informações complementares ou validar as informações recebidas com o objetivo de subsidiar as decisões no âmbito do processo de comunicação de incidente de segurança com dados pessoais*

Restringir situação em que a auditoria possa ser realizada. Ela deve ser o último recurso, depois de a ANPD tentar obter do controlador e não conseguir informação ou não receber informações suficientes.

> ***Art. 19*** *Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, dentre outras:*
> *I - ampla divulgação do incidente em meios de comunicação; ou*
> *II - medidas para reverter ou mitigar os efeitos do incidente.*

Recomenda-se que a Autoridade defina os parâmetros e os critérios para avaliar a gravidade do incidente, conferindo previsibilidade e segurança jurídica para os agentes de tratamento, evitando abusos/arbitrariedades.

Especificamente em relação ao inciso I, embora, no art. 24, a Autoridade tenha se adiantado para dizer que essa ampla comunicação não se trata de sanção de publicização, é importante que o termo "ampla divulgação" seja mais objetivo e sejam estabelecidas as diferenças entre essa medida e a sanção de publicização. Ademais, seria interessante mais informações sobre essa medida a fim de garantirmos que ela irá auxiliar o titular, de fato, e não dar mais insumo aos atacantes (nos casos em que o incidente ainda está acontecendo, por exemplo) e colocar em risco a integridade do titular. Não entendemos que essa medida traz algum tipo de proteção ao titular, além da transparência.

> ***Art. 20.*** *A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, a ser custeada pelo controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.*

Recomenda-se que seja determinado o que poderia ser considerado como “meios insuficientes” para alcance significativo dos titulares de dados afetados.