02 de junho de 2023

Waldemar Gonçalves Ortunho Junior
Presidente, Conselho de Administração
Autoridade Nacional de Proteção de Dados

Re: Consulta ANPD - Regulamentação da Comunicação de Incidentes de Segurança com Dados Pessoais

A BSA | A Software Alliance agradece a oportunidade de fornecer os comentários abaixo em resposta ao projeto de resolução da Agência Nacional de Proteção de Dados (ANPD) sobre a Regulamentação da Comunicação de Incidentes de Segurança com Dados Pessoais.

A BSA é a principal defensora do setor de tecnologia empresarial. Nossos membros estão entre as empresas mais inovadoras do mundo e ajudam a impulsionar a transformação digital, fornecendo as soluções que tornam as empresas e os governos mais competitivos e eficazes, incluindo computação em nuvem, gerenciamento de relacionamento com o cliente, gerenciamento de recursos humanos, gerenciamento de identidade e acesso, análise de dados, manufatura e ferramentas e serviços de infraestrutura.

A BSA compartilha sua preocupação com o crescente número de incidentes cibernéticos, bem como seus impactos em indivíduos, organizações e todo o ecossistema digital. Nós nos esforçamos para enfrentar esses desafios por meio da colaboração público-privada. Como afirmamos no Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda, "Em um mundo em que nem a indústria nem o governo podem, sozinhos, resolver um conjunto de desafios em constante evolução, as parcerias público-privadas provaram ser a abordagem mais eficaz para melhorar a segurança cibernética das organizações e do ecossistema digital".

A BSA aplaude a ANPD por observar no projeto de regulamento que as obrigações de relatar violações de segurança relevantes se aplicam apenas aos controladores de dados. Esse esclarecimento traz segurança jurídica quanto ao papel dos processadores de dados, que devem fornecer aos controladores de dados informações relevantes sobre incidentes de segurança, quando aplicável, mas não devem ser responsabilizados pela notificação à ANPD e aos titulares dos dados.

A BSA oferece os seguintes comentários específicos.

1. **Critérios de notificação de incidentes de segurança (Artigo 5)**

O projeto de regulamento exige que os controladores de dados notifiquem a ANPD quando forem vítimas de incidentes de segurança que possam criar risco relevante ou causar danos relevantes aos titulares dos dados. Um incidente de segurança atingirá esse limite se 1) tiver o potencial de afetar os direitos fundamentais dos titulares de dados e 2) for enquadrado em pelo menos uma das categorias listadas no artigo 5º.

Muitos incidentes podem ser atendidos pelo primeiro requisito mencionado acima, pois muitos incidentes potencialmente impactarão os direitos fundamentais dos titulares de dados, que são definidos amplamente pelo artigo 5º, § 1º, como aqueles que poderiam impedir ou limitar o acesso a um serviço ou causar danos materiais ou morais. Contudo, nem todos os serviços são considerados suficientemente relevantes para serem considerados como tendo um impacto relevante nos direitos fundamentais do titular dos dados. Com base na definição atual fornecida pelo artigo 5º, § 1º, por exemplo, se um titular de dados não puder acessar um serviço não essencial por apenas alguns minutos devido a um incidente de segurança, o incidente será considerado como tendo impactado os direitos fundamentais do titular dos dados, o que não parece sustentar a abordagem ponderada contida no projeto de regulamento. A BSA recomenda, portanto, que o artigo 5º, § 1º, I, seja alterado para incluir apenas incidentes que afetem serviços essenciais.

Para refinar ainda mais o escopo, dado os muitos incidentes que atenderiam ao requisito discutido no parágrafo anterior (mesmo com a melhoria recomendada pela BSA), a ANPD determinou que um requisito adicional precisaria estar presente para que um incidente fosse "relevante" para fins de notificação. A BSA recomenda um maior refinamento do escopo, garantindo que as categorias de risco estejam alinhadas com os riscos reais associados a um incidente de segurança relevante.

A. **Incidentes de segurança incluindo dados referentes a crianças, adolescentes, idosos (artigo 5º, II):** o nível de risco de um incidente de segurança não pode ser determinado apenas pela idade do titular dos dados. Por exemplo, se dois incidentes de segurança têm exatamente as mesmas características, exceto que um deles inclui dados de 30 pessoas com idades entre 25 e 40 anos e o segundo incidente inclui dados de 29 pessoas com idades entre 25 e 40 anos e 1 pessoa com 70 anos, o nível de risco associado aos dois incidentes pode não ser significativamente diferente. Além disso, para que um controlador de dados saiba a idade de um titular de dados, ele precisaria implementar mecanismos complexos de verificação de idade que resultariam na coleta de mais dados do que o necessário para os fins de processamento, aumentando os riscos de privacidade. A BSA, portanto, recomenda a exclusão do artigo 5º, II.
B. **Incidentes de segurança, incluindo dados de autenticação do sistema (artigo 5º, IV):** Incidentes de segurança envolvendo senhas que dão acesso a um sistema não necessariamente criam risco elevado para os titulares dos dados. Por exemplo, se um sistema requer um processo de autenticação de dois ou vários fatores e apenas um conjunto de vários fatores foi comprometido, o resultado do incidente não é do tipo que o ANPD está visando, porque não criaria o mesmo tipo de risco de outros incidentes. De fato, esse cenário demonstra o valor da implementação da autenticação multifatorial. A BSA recomenda a alteração desta disposição para indicar que apenas os incidentes relacionados com os dados de autenticação do sistema que

efetivamente fornecem acesso a esses sistemas estão abrangidos pelo âmbito de aplicação.

C. **Grandes quantidades de dados, (art. 5º, V):** A quantidade de dados envolvidos em um incidente de segurança não determina seu risco. Por exemplo, o risco associado a um incidente que inclui uma grande quantidade de dados pode ser mínimo ou inexistente porque envolveu apenas informações criptografadas. A BSA recomenda que este ponto seja excluído do projeto de regulamento.

2. Calendário da notificação (artigo 6.º)

O projeto de regulamento exige que o controlador notifique a ANPD em até três dias úteis após o conhecimento do incidente de segurança relevante. Embora um prazo de três dias esteja alinhado com as leis de outros países com regulações semelhantes, como a Lei de Relatório de Incidentes Cibernéticos para Infraestrutura Crítica nos Estados Unidos, um prazo arbitrário pode não ser propício para que a ANPD ou as partes afetadas obtenham informações úteis. Dessa forma, para muitos incidentes de segurança previsto projeto de regulamento, uma entidade controladora de dados não saberá informar, com exatidão, os tipos de informações que a ANPD busca, tais como a natureza do incidente ou o número de titulares afetados. Em muitas circunstâncias, um controlador de dados saberá que é vítima de um incidente de segurança, mas trabalhará em seu próprio processo de resposta para proteger os dados de seus usuários e determinar informações sobre o incidente de segurança.

Um cronograma mais flexível para a notificação ajudará a evitar sobrecarregar a ANPD com notificações imateriais e evitará o desvio de recursos da empresa de atividades de resposta que melhorem a segurança e a privacidade.

A BSA recomenda que, dados os desafios da resposta a incidentes, a ANPD permita que as entidades vítimas comuniquem à ANPD no prazo de três dias úteis ou assim que possível, o que aumentará a probabilidade de que uma entidade vítima possa fornecer as informações solicitadas pela ANPD.

3. Comunicação ao Titular (artigo 9.º).

O projeto de regulamento exige que os responsáveis pelo tratamento de dados comuniquem o incidente de segurança ao titular dos dados no prazo de três dias úteis, mas não prevê exceções.

No entanto, notificar os titulares dos dados em um período tão curto pode ser contraproducente. Por exemplo, quando essa comunicação puder exacerbar os riscos para a segurança e a privacidade dos dados do titular dos dados ou interferir com uma investigação da ANPD ou outra investigação criminal, a notificação não deve ser exigida.

Além disso, os responsáveis pelo tratamento de dados podem identificar e responder a um incidente de segurança relevante e evitar, com êxito, maiores riscos de danos para o titular dos dados; caso em que o regulamento deve clarificar que o responsável pelo tratamento de dados não possui a obrigação de notificar o titular dos dados. A título de exemplo, o artigo 34 do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia prevê tais exceções.

A BSA recomenda que a ANPD inclua exceções à exigência de comunicação de três dias com o objetivo de garantir que qualquer comunicação priorize a segurança e a privacidade dos titulares e não prejudique o propósito da regulamentação.

4. Conservação de dados (artigo 10.º)

O projeto de regulamento exige que os dados relativos a incidentes de segurança, mesmo aqueles incidentes que não são considerados significativos o suficiente para desencadear a exigência de notificação, sejam mantidos por 5 anos. Exigir que os controladores de dados retenham os dados cria riscos de privacidade e segurança. Embora, em algumas circunstâncias, esses riscos possam ser compensados por outros benefícios, é pouco provável que seja esse o caso, especialmente para situações em que um incidente não tenha atingido o nível necessário para exigir a notificação. A BSA recomenda que a ANPD reveja seus requisitos de retenção de dados.

5. Auditorias e inspeções (artigo 18.º)

O projeto de regulamento permite que a ANPD "a qualquer momento" inspecione e colete informações para um controlador de dados. O projeto de regulamento não especifica o âmbito de uma inspeção nem o que uma inspeção implicaria. Por exemplo, o artigo 18 poderia ser mal interpretado no sentido de permitir que funcionários da ANPD tivessem acesso às instalações de processamento de dados, o que levantaria preocupações de segurança e privacidade, especialmente quando a parte sujeita à inspeção é uma empresa (business-to-business) que processa dados em nome de vários clientes que não estão implicados na investigação da ANPD.

A BSA recomenda que a ANPD inclua salvaguardas processuais e substantivas, limitando quando e como a regulamentação autorizaria a ANPD a inspecionar dados e garantindo que essas inspeções não criem maiores riscos à privacidade e

Sinceramente,

Antônio Eduardo Mendes da Silva
Country Manager, Brasil
BSA | The Software Alliance