18/05/2023 11:55:29 - EMPRESAS

ARTIGO/PATRÍCIA PECK: SOBERANIA DIGITAL

Em 2019, um grupo de representantes de 28 países se reuniu em Washington D.C para discutir como desenvolver uma Economia Digital confiável e segura, ou nos termos originais em inglês “How to develop a Digital Economy Reliable and Safe?”. Nesta agenda, tomou-se por base três pilares para a análise: 5G, cloud computing e Inteligência Artificial. Ou seja, quais os impactos da junção destes fatores e como os países deveriam desenvolver suas estratégias de “Soberania Digital” para o futuro.

De lá para cá, a discussão desta temática só cresceu de importância e assumiu a pauta prioritária do G-20. Também passou a ser tópico das discussões em Conselhos de Empresa e começou a bater na porta do Judiciário e do Legislativo na medida em que uma das abordagens que fazem parte da gestão de risco cibernético é justamente evitar o excesso de concentração de mercado, ou seja, a melhor prática é “não fique refém de um único fornecedor”.

Além disso, também há nesta cartilha de recomendações para gestores públicos e privados outras orientações, tais como a de garantir sempre a proteção dos dados onde quer que eles estejam, o que quer dizer que a segurança acompanha a informação principalmente em ambientes de “cloud” (nuvem) que provocam fluxos fora do território soberano de um Estado. Se os dados podem parar em qualquer lugar, melhor que estejam com criptografia, para que só sejam vistos por quem seja autorizado (detenha chave de acesso).

Portanto, a definição dos protocolos criptográficos e dos requisitos relacionados à contratação de “nuvem segura” exige ainda a confirmação de que o país onde estiver o ofertante (fornecedor) deva estar sempre, à época da contratação, com compromisso firmado com o país contratante, ou seja, tanto as partes envolvidas como os países devem reafirmar cumprir com as legislações recíprocas, bem como colaborar com autoridades de cada um.

Isso quer dizer que, de tempos em tempos, um determinado fornecedor, por melhor preço que tenha, pode passar a ter restrição de participar de contratos com o Brasil por não atender aos requisitos e protocolos de “soberania digital” brasileiros.

Também faz parte da construção da estratégia de “Soberania Digital” o alinhamento com os princípios de segurança da informação (disponibilidade, integridade e autenticidade), com necessidade de realização de testes de “perda e recuperação de controle” cronometrados e alinhados com SLAs (Service Level Agreements) bem definidos.

No contexto em que vivemos atualmente, é possível, literalmente tirar um país inteiro do ar, com efeitos políticos, sociais e econômicos devastadores. Este tipo de ataque, que pode ser orquestrado por quadrilhas de ciber criminosos ou ciber terroristas, tem se tornado mais comum e exige a realização de exercícios de simulação de sala de crise (também chamada de “war room” para verificar a capacidade de restabelecimento das estruturas críticas, medição de tempos de resposta e avaliação de impactos.

É curioso perceber que a maioria dos gestores e executivos ainda não se deu conta do quanto já estamos vivendo esta realidade e o despreparo atual das instituições. Basta fazer uma pergunta simples: quando você interage com uma IA Generativa, como exemplo, o ChatGPT, onde estão os dados? No Brasil, nos Estados Unidos, na China? E quem pode acessar os dados? Bem, a maioria não sabe responder.

Isso mostra o quanto precisamos investir na construção da estratégia de Soberania Digital do Brasil e trazer mais visibilidade sobre todas estas situações em que fazemos uso de recursos na nuvem e como os dados já param em outros países, de forma desprotegida.

O ponto de atenção continua sendo a mesma pauta na qual pude participar representando o Brasil como especialista em Direito e Cibersegurança em 2019: como usar as tecnologias desenvolvendo economia digital de forma confiável e segura (“reliable and safe”)?

E isso define prioridades, como, por exemplo, a importância da Autoridade Nacional de Proteção de Dados (ANPD) regulamentar o artigo 46 da Lei Geral de Proteção de Dados Pessoais (LGPD), conforme previsto em seu § 1º, para detalhar os padrões técnicos mínimos de segurança de dados. Sem isso, todos os dias, enfrentamos licitações cujos editais têm dificuldade de exigir os requisitos seja da LGPD ou de Soberania Digital, principalmente os relacionados à proteção e à segurança de dados.

Infelizmente, a pauta sobre segurança sequer entrou na agenda regulatória 2023-2024 da ANPD e o Conselho Nacional (CNPD) está inativo, contrariando previsão de seu Regimento e da própria lei para que seja ouvido em matéria técnica-regulatória. Não há mais tempo a perder. O Brasil e o povo brasileiro não podem ficar expostos a toda sorte de vazamentos e sequestro de dados, tampouco refém do exercício de posição dominante de mercado por concentração excessiva neste ou naquele fornecedor de tecnologia.

Dra. Patricia Peck, CEO e sócia fundadora do Peck Advogados, Conselheira Titular do Conselho Nacional de Proteção de Dados (CNPD) e Professora de Direito Digital da ESPM.