

Por Cesar Luiz Danieli (*)

Cada vez mais, observamos a escalada da informação e do conhecimento, assumindo como item essencial de matéria prima da economia. No passado, outros itens, tais como o domínio da navegação, e o carvão, dentre outros itens, foram essenciais na formação da economia, e hoje podemos dizer que a detenção de dados e da informação exerce o papel de motor primordial dos mercados.

A partir do pressuposto, e mais evidente, nas operações de previdência complementar e de seguros, onde é primordial deter dados e informações, os quais são utilizados para analisar o risco, elaborar os cálculos atuariais e estabelecer os prêmios (no caso de seguros) e contribuições (no caso de planos de benefícios previdenciários e de saúde) de acordo com as características e extensão dos riscos assumidos pelas organizações securitárias. Assim, as entidades de previdência complementar – EFPC, operadoras de planos de saúde e seguradoras, a fim de conseguir o máximo de informações possível a respeito das pessoas, se valem da coleta e da análise de dados e informações pessoais, uma vez que é só através do conhecimento de informações detalhadas a respeito de seus participantes e segurados que essas organizações securitárias podem desenvolver adequadamente as suas atividades.

Com a elevada necessidade de especificações e conhecimento de hábitos, do estado de saúde, de bens materiais e demais necessidades pessoais dos segurados e participantes, as organizações securitárias detêm vasto conhecimento e guarda de dados pessoais tendo aumentado cada vez mais as preocupações com a proteção e privacidade dos mesmos. Uma das principais medidas para gerenciar estes riscos, que descrevemos neste artigo, é a implantação de política de proteção e privacidade de dados pessoais com a devida ciência e concordância dos respectivos usuários.

Essa discussão torna-se importante, em especial no âmbito das organizações securitárias, pois detêm grande quantidade de dados e muitos que se constituem de dados de sigilo pessoal, como por exemplo, a informação de ser ou não portador de necessidades especial ou de doenças, dentre outras informações pessoais sigilosas, constituindo-se, desta forma uma urgente necessidade de estabelecer uma política de privacidade e proteção de dados pessoais, bem como de comitê de privacidade e delegado para a proteção dos dados pessoais como responsável pela implementação e verificação desta política de privacidade. Apesar de não haver exigência legal, ainda, em constituição de política de proteção de dados pessoais, podemos encontrar várias empresas e em especial seguradoras que, de forma voluntária, já contam com sua política de proteção de dados pessoais.

Mundialmente, a legislação caminha para a instituição de regras, a exemplo da Diretiva n. 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 e alterações posteriores, proposto também, no caso brasileiro, o anteprojeto de lei proteção-dados-pessoais, com o objetivo de compreender várias regras que regulam a coleta, utilização, comunicação e cuidados de dados pessoais. A legislação reconhece tanto os direitos dos indivíduos para proteger seus dados pessoais, incluindo os direitos de acesso e correção, e as necessidades das organizações para coletar, utilizar ou divulgar dados pessoais para fins legítimos e razoáveis.

Em termos gerais, uma política de privacidade e proteção de dados pessoais de organizações securitárias estabelecem a salvaguarda do direito à proteção de todos os dados pessoais, nos termos da legislação (Proteção dos Dados Pessoais), que sejam prestados voluntariamente pelo utilizador e autorizados por este (por serem necessários e fundamentais ao funcionamento dos programas de consulta, simulação, cálculos e aos contatos por via eletrônica), os quais deverão ser tratados de forma confidencial, nos termos da legislação em vigor, pela organização, através de qualquer funcionário ou representante por esta autorizados para este efeito. Desta forma, geralmente a política contém:

a) As políticas gerais;

- b) Tratamento das informações;
- c) Relacionamento com terceiros;
- d) Segurança;
- e) Direitos; e,
- f) Recomendações

Além disso, deve-se deixar configurado, também, que os dados e parte deles, assim como os que se venham a gerar em caso de sinistros e de eventos cobertos, poderão vir a ser cedidos a organismos públicos e privados relacionados com as atividades de seguros, previdência e de planos de saúde suplementar, com fins estatístico-atuariais e de prevenção de fraude.

As organizações, que têm a informação pessoal como uma fundamental ferramenta para o exercício de suas atividades, devem estar atentas às prováveis mudanças no cenário nacional de proteção de dados, sendo recomendável, inclusive, que se antecipem a essas questões e elaborem uma política específica para as peculiaridades do tratamento de dados nas suas atividades, inclusive com salvaguardas quando por necessidade ocorrer a transferência para outras empresas.

Assim, depreende-se que um sistema de base de dados que contenham informações pessoais utilizados pelas organizações securitárias devem ser planejados com a natureza e a complexidade dos produtos, planos de benefícios, atividades, processos e seus sistemas, bem como considerar os requisitos de confidencialidade e possuir uma equipe de especialistas multidisciplinares a seu lado para cumprir as múltiplas missões de sua competência, que poderá ser dentre outros especialistas os escritórios de Consultoria Atuarial com expertise nos aspectos técnicos e legais que revestem a matéria.

(*) **Cesar Luiz Danieli** é Atuário e Diretor de Previdência, Saúde e Seguros da GAMA Consultores Associados.

Fonte: [GAMA Consultores Associados](#), em 23.03.2015.