Por Eduardo Tardelli (*)

O ano de 2018 foi marcado por diversos escândalos no mundo *online* envolvendo compartilhamento de informações pessoais de plataformas sociais como, por exemplo, os 50 milhões de americanos que tiveram dados utilizados de forma irregular pelo Facebook e acessados pela empresa de consultoria Cambridge Analytica; ou, em outra ocasião, o vazamento de elementos de 87 milhões de pessoas por essa mesma rede social, das quais 443 mil eram brasileiros.

Seja por problemas nas plataformas, fraudes no armazenamento das informações ou ataques de hackers, esses vazamentos indevidos violam a Constituição Federal, já que expõem a privacidade garantida pela lei ao cidadão, além de contrariar o Marco Civil da Internet (Lei 12.965, de 2014) e o Decreto 8.771, de 2016, que restringem provedores de aplicativos de repassar dados dos usuários a terceiros.

A cibersegurança é, em resposta, um mercado crescente, principalmente porque grande parte dos serviços, sociais ou empresariais estão hospedados em nuvens, junto com as informações mais valiosas. Assim, as marcas precisam assegurar essa informação de algum modo, e a cibersegurança é a única forma de antecipar muitos desses riscos. O caminho é (e sempre será!) a prevenção.

Os criminosos, com diferentes experiências e conhecimentos, têm se adaptado e unindo-se para vender componentes de ataques por módulos, além de fortalecer o mercado de malware. O perigo instaura-se nessas quadrilhas cibernéticas, que tendem estar associadas com crimes de lavagem de dinheiro, fraudes institucionais e bancárias, técnicas de evasão e explorações de vulnerabilidades.

Portanto, todas as empresas devem preocupar-se com seus dados e antecipar-se aos riscos, formando equipes responsáveis pelo desenvolvimento de soluções internas e externas que tragam mais estabilidade e segurança aos seus sistemas, e consequentemente aos seus dados. Os cibercriminosos estão sempre atrás de informações sensíveis, que são as mais valiosas para os negócios, e a mais importantes para eles para cometerem fraudes, realizar compras indevidas e muitas outras ações ilícitas.

Vale lembrar que os cibercriminosos tornam-se cada vez melhores em infiltrar-se nos sistemas em busca dessas informações sensíveis e não seria diferente conosco. Por isso, adequar-se à Lei Geral de Proteção de Dados é transformar o negócio em um gerador e armazenador de dados cuidadosos, trazendo uma postura muito mais ativa diante deste problema. Pense nisso!

(*) **Eduardo Tardelli** é CEO da upLexis, empresa de software que desenvolve soluções de busca e estruturação de informações extraídas de grandes volumes de dados (Big Data) extraídos da internet e outras bases de conhecimento.