Por Rodrigo Marques (*)

A ampla utilização da internet por pessoas, empresas, organismos e governos possibilitou uma integração sem precedentes, fazendo com que as fronteiras geográficas que existem fisicamente não mais sejam relevantes diante de um atributo intrínseco às informações digitais – elas transitam praticamente livres pela rede mundial de computadores.

Esta nova economia tem como seu principal ativo os dados pessoais de todas as pessoas que acessam a internet e consomem, de alguma forma, os mais variados produtos e serviços que lá estão disponibilizados.

No Brasil, em 14 de agosto de 2018, houve a promulgação da **Lei 13.709**, conhecida largamente como LGPD – Lei Geral de Proteção de Dados que, ainda que não esteja em vigor, já impõe para as empresas brasileiras de todos os tamanhos, modelos de negócios e áreas de atuação, o dever de

entrar em conformidade com seus 65 artigos. Afinal, no mínimo, deverão ser protegidos e tratados os dados pessoais dos sócios das empresas e seus funcionários.

A nova normativa traz aos holofotes a questão de proteção de dados e privacidade exigindo das empresas que revejam seus processos internos de tratamento de dados desde o momento inicial da coleta, seja pela forma que for, até a exclusão dos mesmos. Tudo isso deve ser feito sem deixar de tomar cuidado com todos os tratamentos feitos no meio do caminho.

Fundamental é perceber que a lei não trata apenas dos dados pessoais on-line, que transitam pelo meio eletrônico, mas também dos dados pessoais que se encontram em meio físico, no bom e velho papel.

A tarefa de aplicar a conformidade legal às empresas é árdua e complexa, envolvendo, necessariamente, o esforço coletivo de toda organização, partindo desde a presidência e diretoria, até a operação como um todo.

Frequentemente percebe-se, na prática, que as empresas não conseguem verificar com 100% de clareza todos os canais de entrada de dados e, muito menos, todos os tratamentos que ocorrem, bem como as pessoas que manipulam os dados dentro da companhia.

Também é difícil saber, sem uma auditoria, o real ciclo de vida desses dados dentro das empresas, que muitas vezes acabam armazenando essas informações em locais que não são tão seguros, como as caixas de e-mail de seus colaboradores, dispositivos de armazenamento portáteis - como HDs externos e pen drives - ou até mesmo celulares pessoais daqueles que colocam seus e-mails corporativos ou acessos a nuvem corporativa da empresa para acessá-los remotamente - invariavelmente realizam um download dessas informações.

Sendo assim, a solução não é coibir tais comportamentos que já são absolutamente rotineiros no ambiente corporativo, mas sim instaurar na empresa programas de Compliance Digital e Política de Segurança da Informação. Reformatar os processos internos sob a lógica do *Privacy by Design* e *Privacy By Default*, ambas metodologias determinadas pela própria legislação pátria, também é recomendado.

(*) **Rodrigo Marques** é sócio da área de Direito Digital e Tecnologia do Marins Bertoldi Advogados, Professor, Especialista em Direito Digital e Compliance e Pós-Graduando em CyberSecurity.

(07.03.2019)