Por Karollyne Uggeri (*)

É muito importante que a empresa tenha o **Compliance Digital**, cuja função essencial é a análise de riscos e a adoção de medidas preventivas para adequação da empresa às regras aplicáveis às tecnologias da informação.

A palavra Compliance de origem inglesa (*to comply*) significa agir de acordo com uma regra, ou seja, "estar em Compliance" é estar em conformidade com leis e regulamentos internos e externos, por meio de esforços sistemáticos que visam prevenir, detectar e responder a possíveis problemas de desvio entre as normas estabelecidas e a prática da empresa.

Nesse sentido, Compliance é um conjunto de regras internas que regulam as mais diversas atividades da empresa para que ela esteja em consonância com as normas vigentes e aplicáveis àquelas atividades por ela desenvolvidas.

Ao "estar em Compliance" com as boas práticas e padrões existentes, isto é, coibindo comportamentos futuros inadequados que podem macular a sua reputação, a empresa se fortalece e recebe o reconhecimento do mercado. Além da vantagem competitiva, a empresa recebe outros benefícios como: desconto em linhas de crédito; valorização da organização; melhor retorno dos investimentos, entre outros.

Dentro do cenário mundial de combate à corrupção, é uma necessidade atual de toda empresa (i) zelar pela imagem limpa e desvinculada de atitudes ilícitas pautando-se por elevados padrões éticos e morais; (ii) manter as informações seguras; (iii) mostrar, e comprovar, para o mercado que "está em Compliance".

Isto porque, todos os agentes da sociedade, cada vez mais, dão preferência a se relacionar com empresas éticas. Além disso, também é muito importante que a empresa tenha o Compliance Digital, cuja função essencial é a análise de riscos e a adoção de medidas preventivas para adequação da empresa às regras aplicáveis às tecnologias da informação.

Inclusive, depois da onda de ataques cibernéticos ocorrida em escala mundial no final de 2017, que atingiu empresas do setor privado e órgãos governamentais em pelo menos 74 países, incluindo o Brasil, a importância das práticas de Compliance Digital, nas esferas pública e privada, para a proteção de dados ganhou maior relevo, pois o referido ataque cibernético alertou o mercado para a insuficiência de cuidados relativos à segurança das informações.

Como se vê, a falta do Compliance Digital pode representar impedimento à operação da empresa e, até mesmo, um risco à sua saúde financeira.

Destarte, imprescindível estar sob a ótica do Compliance Digital, o monitoramento e o controle (**i**) das ferramentas de comunicação e (**ii**) dos dados corporativos, que podem estar armazenados em qualquer lugar: no servidor da companhia, no smartphone ou em uma plataforma qualquer de computação em nuvem, bem como (**iii**) das situações em que os dados podem ser facilmente perdidos e ocasionarem um grande problema para a empresa.

Nesse sentido, destacam-se algumas medidas importantes dentro de um programa de Compliance Digital, tais como: (**i**) a realização de auditoria prévia para identificar as tecnologias presentes no cotidiano da empresa que necessitam de maior atenção; (**ii**) verificação da proporção entre as licenças de uso contratadas e a quantidade de usuários habilitados; (**iii**) a adequação das políticas de privacidade e termos de uso dos canais web disponibilizados pela empresa às legislações específicas, tais como o Marco Civil da Internet, Código de Defesa do Consumidor, entre outras; (**iv**) a implementação de políticas internas de gestão dos recursos de tecnologia da informação. Por meio desses instrumentos a empresa poderá exigir a aplicação adequada de seus recursos tecnológicos e coibir abusos ou desvios que possam comprometer a atividade empresarial e a sua

imagem.

A instauração de políticas de Compliance Digital contribui para um ambiente empresarial mais seguro e eficiente, bem como para a construção de relações transparentes com fornecedores e clientes. Além disso, viabiliza a responsabilização subsidiária dos agentes responsáveis por eventuais ilicitudes na utilização do parque tecnológico da empresa.

No entanto, é importante destacar que a implementação do Compliance Digital por si só, não é suficiente à proteção da empresa, sendo necessária, ainda, a revisão constante das políticas de controle e análises de riscos por meio de uma fiscalização eficiente.

Contudo, é inegável que a sua implementação demonstra que a empresa trata com seriedade a proteção privada dos dados dos seus clientes, atua no combate à corrupção e está adotando padrões éticos e morais perante a sociedade e a justiça.

(*) **Karollyne Uggeri** é advogada do escritório Nelson Wilians & Advogados Associados, especialista em Direito Corporativo (IBMEC/RJ).

Fonte: Migalhas, em 01.03.2018.