

Por Helio Ferreira Moraes (*)

Para obedecer às leis, preservar a reputação ou pela nobre motivação a fazer a coisa certa, as empresas têm investido cada vez mais em compliance. Mas, afinal de contas, o que é isso? De uma maneira bastante simples, o compliance é o cumprimento, pelas empresas, de todas as normas, regras e legislações aplicáveis ao seu setor de atuação. Podem incluir questões trabalhistas, fiscais, contábeis, financeiras, ambientais, previdenciárias e éticas. E além de normas externas, a empresa pode criar suas próprias políticas e diretrizes alinhadas a seus valores e objetivos.

Com a evolução dos negócios, o compliance tradicional foi sendo ampliado, passando a compreender qualquer atividade empresarial que demande padronização e transparência. Processos internos, metodologias de trabalho, políticas de estoques, estratégias de gestão de pessoas e harmonização contábil passaram a seguir regras claras e, acima de tudo, inexoráveis.

Do ponto de vista legal, também ocorreram diversos fatos recentemente no Brasil que impulsionaram o interesse pelo assunto, como a Lei Anti-Corrupção em 2013. Ela adotou diversos princípios de países mais experientes no assunto como o UK Bribery Act do Reino Unido e o FCPA (Foreign Corrupt Practices Act) americano. Essas leis internacionais já obrigavam as empresas a criar programas de prevenção e de monitoramento constante de suas atividades internas e externas. Além disso, investigações como da Operação Lava Jato passaram a colocar em xeque empresas e setores da economia brasileira que reiteradamente operavam mediante práticas ilegais de relacionamento entre clientes e fornecedores. Algumas dessas empresas foram verdadeiramente varridas do cenário de negócios, tendo que demitir funcionários e fechar as portas.

Mas o mundo corporativo tem o mesmo rigor quando o assunto é uso de computadores, gadgets e internet?

Nos últimos anos, foram criadas leis que abordam vários aspectos da internet, como as regras do Marco Civil, a proteção contra crimes da Lei Carolina Dieckmann e a lei que previne o bullying. Sem contar os inúmeros projetos de lei que pretendem criar novas regras de proteção de dados, combate a crimes e injeção de recursos financeiros para melhor aparelhamento de autoridades investigativas.

Enquanto isso, as empresas fornecem notebook, smartphone e infraestrutura para o empregado trabalhar como o esperado. Ele também pode desempenhar suas funções em sistema de home office, usando seus próprios equipamentos. Ou pelo menos chegar em casa e dar aquela checada rápida nos e-mails depois do expediente. E que tal levar ao trabalho o seu próprio dispositivo, no sistema de BYOD (Bring Your Own Device)? E levante a mão quem nunca usou o computador da empresa para baixar uma foto do fim de semana.

Como regular essa mistura de mundo privado com profissional? É aí que entra o e-Compliance.

Esses comportamentos entraram nas empresas da mesma maneira em que surgem as tecnologias disruptivas: rapidamente e sem se preocupar com formalidades ou burocracias. É com essa realidade já instaurada que as empresas devem equilibrar a segurança de seus processos e a manutenção de um ambiente fértil para inovação. É preciso decidir quando um recurso deve ter seu uso restringido ou encorajado. Para isso, cada empresa precisa ter sua própria cultura levada em consideração e, assim, rever as políticas de gestão de pessoas com novos manuais de conduta.

Com o bonde já andando, as empresas devem avaliar os riscos operacionais trazidos por essas novas formas de trabalhar, começando pela revisão de suas políticas de segurança da informação. No começo dos anos 2000, quando surgiu a preocupação de estabelecer regras explícitas de uso de recursos tecnológicos, o foco estava no uso do computador na mesa do usuário. Para coibir o uso das incipientes redes sociais, bastava bloquear o acesso pela máquina. Hoje, se o desktop tem

algum bloqueio, o empregado saca seu celular particular e acessa o que quiser. E mais: se por um lado as redes sociais podem ser inimigas da produtividade, elas também podem ser excelentes ferramentas de integração profissional e de divulgação de ações internas e externas da empresa.

O tratamento de dados – tanto os relacionados a rotinas internas como aqueles que compõem big data de grande valor comercial – também deve ser feito de forma responsável e observando protocolos que garantam integridade e confidencialidade. Nossos legisladores passaram a se atentar aos riscos envolvendo o uso irresponsável de dados e já estamos observando movimentações para a propositura de projetos de lei que trarão regras para organizar esse mercado.

O e-Compliance surge, então, como uma abordagem especializada para assegurar que a empresa esteja em conformidade com essas novas práticas tecnológicas. Veja algumas medidas de prevenção de risco:

- **Atualização das regras:** Para empresas que no passado já criaram suas regras de conduta, é preciso verificar se elas ainda são válidas à luz do Marco Civil da Internet. Deve-se avaliar se os seus termos de uso e políticas de privacidade cobrem as ferramentas mais modernas e estão compatíveis com a proteção do negócio digital. Dá-se atenção especial às práticas de coleta e uso de dados, condições de guarda de logs de usuários, segurança da informação e a postura perante autoridades governamentais na hipótese de solicitação de dados.

- **Adaptação a novas tecnologias:** Os novos negócios digitais são aderentes às diversas leis do Brasil? Essa reflexão exige foco, por exemplo, nos direitos do consumidor no e-commerce, avaliando se, por exemplo, um produto de IoT (Internet das Coisas) infringe alguma legislação nacional. Também merecem atenção os novos meios eletrônicos de pagamento (que já estão sujeitos a regras e obrigações perante o Banco Central); as condições para tratamento de dados obtidos diretamente do cliente ou de terceiros; a neutralidade de tráfego consagrada pelo Marco Civil; o cuidado para que ações de marketing digital não violem direitos fundamentais, como ao de privacidade e a realização de crowdfunding e de equity crowdfunding com o cuidado de não se infringir nenhuma lei.

- **Uso responsável das redes sociais:** Verificação dos sites, portais, aplicativos, estratégias de promoções comerciais e ambientes de negócios nas redes sociais para adequação de eventuais inconformidades. Essas novas interfaces com empregados e clientes podem gerar conflitos ou abrir as portas da empresa para vários tipos de ataques. As equipes devem estar prontas para lidar com situações inesperadas que exijam respostas rápidas e à altura do dinamismo das redes sociais. Os prejuízos podem ir além no mensurável objetivamente: é só pensar nas empresas que, por simples deslize de um profissional ou por má conduta institucionalizada, têm sua reputação destruída por escândalos online.

- **Adequação trabalhista e fiscal:** Verificação se as práticas trabalhistas e fiscais estão compatíveis com as legislações aplicáveis aos novos negócios digitais. Atenção especial ao uso de softwares e dispositivos da empresa ou particulares no ambiente corporativo, inclusive com a previsão de regras específicas para home office.

- **Conscientização dos empregados:** Atualização frequente sobre as novas leis que impactam o negócio; ações de prevenção à pirataria e ao uso não autorizado de conteúdos e imagens; cuidados na mineração de dados e no tratamento de informações pessoais e capacitação para impedir que falhas humanas facilitem ações criminosas, como o ransomware e outros malwares criados para roubar senhas, destruir dados, promover produtos ou sequestrar sistemas em troca de pagamento de resgate.

Está achando essa posição alarmista ou exagerada? No dia 18 de maio desse ano, um homem teve seu notebook furtado enquanto esperava um taxi no aeroporto Santos Dumont, no Rio. Prejuízo de 2 ou 3 mil reais? Não só isso. A vítima era um grande pesquisador do vírus da zika e na máquina estavam salvos estudos sobre uma nova droga, com imagens e informações de pacientes

infectados. Os dados não tinham back-up.

Como a sua empresa e seus empregados estariam preparados para uma situação dessas?

(*) **Helio Ferreira Moraes** é advogado e engenheiro eletrônico formado pela USP.

Fonte: [Canaltech](#), em 27.05.2016.