RESUMO EXPANDIDO

COMPLIANCE EM POLÍTICAS DE PRIVACIDADE E CONTROLE DE DADOS

AUTORA: Bianca Coronetti Farenzena
CO-AUTORA: Laura Covatti dos Santos
ORIENTADORA: Maira Angélica Dal Conte Tonial
UNIVERSIDADE: Universidade de Passo Fundo
EIXO TEMÁTICO: Privacidade, liberdade e direito

INTRODUÇÃO

O instituto de compliance surgiu no século XX, como uma medida de combate à corrupção empresarial, vez que essa se difundiu a nível global e tornou-se um problema governamental. Consolidado como um conjunto de normas e regras que visam garantir a obediência a parâmetros normativos estabelecidos (a nível interno com o regulamento de uma empresa, a nível externo com a legislação do país), abrange todas as esferas, como por exemplo, a "financeira, ambiental, ética, trabalhista, previdenciária, fiscal, contábil." (FERREIRA, 2018, p. 164).

Com o desenvolvimento e aprimoramento dessa ferramenta, além da já esperada redução da corrupção se deram outros efeitos. Entre eles, destacou-se a possibilidade da proteção da privacidade de dados - questão que atualmente é motivo de grande controvérsia e debate. Assim, mediante a urgência do tema, objetiva-se compreender o mecanismo de compliance como auxiliar das políticas de privacidade.

...

Um programa de compliance compreende três fases: prevenir, detectar e remediar (FERREIRA, 2018, p. 164); sendo prevenir o pilar de maior protagonismo. Em relação a constante violação à privacidade de dados, prevenir vem a ser justamente a solução necessária. Assim, não sendo possível separar o ramo empresarial das políticas de privacidade

e da proteção de dados (incluindo-se tanto o controle de dados dos clientes armazenados, quanto os dados da própria empresa e seus funcionários), por meio do método procedimental dedutivo e da análise bibliográfica e de dados, é possível compreender a necessidade do compliance como ferramenta de controle de privacidade e controle de dados.

Os programas (ou planos) de compliance são desenvolvidos por *chief compliance officers* – profissionais especialistas em compliance (FERREIRA, 2018), que adequando-se as necessidades da empresa criam um código a ser seguido por todos os colaboradores. Esse código deve ser composto de um conjunto de normas, que sempre guiadas pela ética devem estar em conformidade com a legislação de onde a empresa se estabelece.

As regras, que vão abordar todas as áreas, devem se preocupar com diversas questões para obter resultados em relação a privacidade e ao controle de dados. Inicialmente é necessário o investimento em um sistema de cibersegurança e privacidade de dados, de modo que garanta o resguardo das informações da empresa e de seus funcionários.

Gutterman (2018), renomado consultor jurídico e comercial, apresenta alguns passos a serem considerados para a construção do plano de compliance no que concerne a dados e privacidade. Deve-se realizar uma análise acerca do fluxo dos dados não públicos recebidos pela empresa e como se dá o acesso a eles (GUTTERMAN, 2018). Esse acesso deve ser acompanhado de uma responsabilização gerencial, devem ser considerados os riscos de privacidade de dados, elaborando-se um plano que aborde isso (GUTTERMAN, 2018).

O programa deve incluir formação educacional para os colaboradores da empresa, entender e levar em consideração a legislação relativa a proteção de dados e privacidade, incluir notificações sobre incidentes relativos ao assunto, estabelecer políticas disciplinares e ainda, garantir a comunicação da política de privacidade e controle de dados para "importantes stakeholders, incluindo funcionários, clientes, parceiros comerciais, órgãos financeiros e reguladores." (GUTTERMAN, 2018).

A aplicação correta de um plano de compliance irá beneficiar tanto a empresa quanto os seus clientes, de modo que, estes terão a garantia de que os dados coletados pela empresa serão submetidos a um tratamento ético sem ter a sua privacidade violada.

A empresa por sua vez, trabalha com menor risco de ataques de hackers, reduz custos que poderiam ser gerados na correção de problemas, aumenta sua confiança no mercado, e ao prevenir o equivocado tratamento de dados reduz a chance de futuras condenações penais por crime de violação à privacidade.

CONSIDERAÇÕES FINAIS

A partir do observado, torna-se possível visualizar o compliance como uma estratégia eficaz no controle de dados e de políticas de privacidade. A ferramenta garante segurança ao cliente em relação à proteção de seus dados, e para a própria empresa, a qual estará protegida de ataques cibernéticos e, consequentemente, estará menos propensa a futuras condenações por crimes de violação a privacidade.

REFERÊNCIAS

FERREIRA, Fábia Duarte. A prática do compliance como um instrumento empresarial anticorrupção para preservação das empresas. **Revista de Direito Bancário e do Mercado de Capitais**, São Paulo, vol. 81/2018, p. 161 – 178, jul/set, 2018.

GUTTERMAN, Alan. Como criar um programa de Compliance sobre privacidade e segurança de dados. **Thomson Reuters**, 09 fev. de 2018. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/blog/como-criar-um-programa-compliance-sobre-privacidade-seguranca-dados.html. Acesso em: 20 de out. de 2019.