

O CERNE DA QUESTÃO DA TRANSFERÊNCIA DE DADOS PESSOAIS:
UMA QUESTÃO DE CULTURA

CLÁUDIA FERNANDES MARTINS

Muito se tem falado sobre a divulgação de dados pessoais pelo Município de Lisboa e sobre a legalidade de uma possível decisão de exoneração do Encarregado de Proteção de Dados, pelo que não vamos entrar aqui pela polémica política ou mesmo sobre a legalidade de uma eventual exoneração do Encarregado de Proteção de Dados do município.

Este artigo não trata, portanto, da transferência de dados pessoais pela Câmara Municipal de Lisboa, nem do papel do Encarregado de Proteção de Dados (*Data Protection Officer – DPO*) na comunicação de dados pessoais de ativistas russos à Embaixada da Rússia.

Importante é perceber como podem acontecer estas coisas. Por que razão organizações públicas e privadas usam e abusam dos nossos dados pessoais e faltam ao respeito a regras jurídicas claras em matéria de cumprimento e conformidade (*compliance*), em matérias de ética e responsabilidade social e ambiental.

O objetivo deste artigo é responder à pergunta: o que falta e o que pode ser feito para que estas situações não se repitam.

Parece-nos que o que está em causa é, sobretudo, a falta de “cultura” das organizações. Ou seja, muitas organizações públicas e privadas habituaram-se a fazer o que sempre foi feito, porque sempre foi feito assim, o que lhes dá uma ilusão de segurança, que é, na verdade, uma falsa segurança.

O facto de ter sido sempre assim, feito pelas mesmas pessoas ou por outras que as antecederam na função, acabando por se transformar num processo mecânico, sem qualquer espírito crítico (ou autocrítico), não está bem e acaba por contaminar, como um vírus silencioso, a organização.

As questões associadas à proteção de dados pessoais (que sempre existiram, mas para as quais as pessoas não estavam alerta ou não lhes davam a devida importância) são propícias a encaixar-se nesse padrão de comportamento tão recorrente dentro das organizações, muitas delas, parecendo estar sufocadas ou embrenhadas nos seus próprios procedimentos, sem nunca fazer sequer uma autoavaliação, para já não falar da falta de avaliações independentes.

A implementação do Regulamento Geral de Proteção de Dados (RGPD) não é uma tarefa fácil e deve ser transversal a todas as organizações – “de fio a pavio” –, não se podendo ficar pela publicação de um conjunto de políticas e códigos e por alterações de fachada. Nem tão-pouco são aconselháveis alterações profundas sem qualquer adesão ao contexto da organização ou sem um verdadeiro envolvimento dos colaboradores.

De qualquer forma, esta situação nunca poderá ser resolvida por uma só pessoa, sem a participação ativa e proativa dos demais colaboradores e sem que a organização esteja ciente ou preparada para alterar padrões de comportamento e para mudar de vida. E não estamos a falar de uma mudança necessariamente brusca, mas ainda assim de uma mudança radical! Claro que, como todos sabemos, falar em mudança assusta!

Isto para dizer que um *Data Protection Officer* (DPO) não é um super-homem que vem salvar a organização dos vilões e da inércia dos demais colaboradores. Há que ter em atenção que, muitos vezes, a função de DPO é desempenhada por colaboradores da própria organização, que acumulam essa função com outras funções que já desempenhavam

originalmente e que por uma questão de necessidade (ou, melhor, de imposição legal) e de poupança de recursos se veem obrigados a aceitar. Muitas vezes o papel dos restantes colaboradores é inexistente em matéria de proteção de dados, porque, como dizem e se convencem, a proteção de dados nada tem que ver com eles (por ser da competência do DPO), quando não deve ser só da competência do DPO. Assim, a própria organização corre o sério risco de acabar por falhar. E, sem dúvida, que, desta forma, todos falham.

A função de DPO é difícil e exigente. Os DPOs têm de ter experiência, têm de ter formação, têm de se atualizar permanentemente, têm de ter ajuda externa, têm de ter a colaboração, o respeito e a ajuda dos demais colaboradores da organização e têm de ter “poder” para mandar fazer ou impedir que se faça.

Atenção que as questões de cumprimento e conformidade não se circunscrevem apenas à proteção de dados pessoais, ainda que a este nível até deveria ser mais fácil entender a relevância do tema, pois, todos somos titulares de dados pessoais, pelo que, mais cedo ou mais tarde, cada um de nós até poderá ser afetado por uma qualquer inércia nesta matéria.

Esta inércia é muito comum quando procuramos apurar o nível de cumprimento e conformidade (*compliance*), ou, melhor, o seu estado de desenvolvimento. Muitas vezes, esse estado é precário, ainda que se crie a falsa ilusão que assim não é, pois, a organização até tem um código de conduta e de ética, várias políticas, processos e procedimentos em curso. A organização até acaba por se convencer que está a fazer tudo bem, pois nunca houve uma situação de incumprimento grave ou muito grave; até ao dia...

Um dos erros mais comuns é pensar que uma cultura da organização surge por magia de códigos e políticas copiadas de manuais de outras organizações mais evoluídas com uma revisão superficial, mas não deve ser assim.

Uma cultura de ética e de conformidade decorre, em primeira linha, da intenção da organização em fazer bem, em fazer o que está certo, da consciência de que há sempre margem para melhorar e que, para isso, é preciso contar com as pessoas – não daquele colaborador em particular ou apenas da direção de topo –, mas de todos. Mais: é preciso ter a abertura para se aceitar ser sujeito a um escrutínio verdadeiramente independente para que as organizações não estagnem nem perpetuem os mesmos erros. É preciso cultura....

8 de julho de 2021

© 2021 MACEDO VITORINO