

# O compliance e o tratamento de dados nas relações laborais

Por **PEDRO PINTO BENTO**



Advogado na Aguiar-Branco & Associados

AO CONTROLO SOBRE OS DADOS PESSOAIS, cada vez mais efetivo e tecnicamente ilimitado, alia-se a circunstância de muitos dos aparelhos utilizados para a recolha desses dados serem tecnicamente invisíveis para os titulares dos dados.

O que tudo determinou a necessidade de criação de regras e limites jurídicos, tanto para regular esta capacidade, cada vez maior, de controlo das organizações sobre os dados pessoais, como para regimentar a aquisição, transmissão e difusão de dados pessoais. Acontece que nem tudo o que é tecnologicamente executável é juridicamente tolerável.

Foi neste circunstancialismo que surgiu o Regulamento Geral de Proteção de Dados (“RGPD”) e, posteriormente, a nossa Lei n.º 58/2019 de 8 de agosto (“Lei de Proteção de Dados” ou “LPD”).

O tratamento de dados pessoais é essencial na relação de trabalho. A dificuldade não está no tratamento desses dados, mas nos limites que são impostos às possibilidades técnicas ilimitadas de tratamento e de controlo dos empregadores sobre os dados dos trabalhadores. Esses limites passam pelos princípios gerais que enformam o tratamento de dados pessoais previstos no RGPD, os artigos 17.º a 22.º do Código do Trabalho (CT) e, agora, as disposições da LPD, mormente o seu art. 28.º.

A LPD tem implicações na relação de trabalho, destacando-se as seguintes:

1. Os dispositivos de geolocalização, videovigilância, audiovigilância ou radiofrequência devem ser considerados como meios de vigilância à distância, pelo que só podem ser utilizados pelos empregadores com a finalidade de proteção e segurança de pessoas e bens e nunca para controlar o desempenho profissional dos trabalhadores (cfr. art. 28.º, n.º1 LPD, art. 4.º RGPD e art. 20.º CT).
2. Os meios de vigilância à distância não podem ser utilizados na vida extraprofissional dos trabalhadores (princípio da proporcionalidade).
3. O empregador não pode utilizar os dados obtidos por meios de vigilância à distância para

finalidades disciplinares, a não ser que sejam simultaneamente ilícitos penais (cfr. art. 28.º, n.º 4 e 5 LPD).

4. Em regra, o consentimento do trabalhador não releva como condição de licitude de tratamentos dos seus dados pessoais (cfr. art. 28.º, n.º3 LPD).
5. O empregador só pode tratar dados biométricos dos seus trabalhadores para (i) controlo de assiduidade e (ii) controlo de acesso às instalações (cfr. art. 28.º, n.º 6 LPD).

Com o novo modelo de supervisão administrativa no que ao tratamento de dados pessoais respeita consagrado pelo RGPD, as organizações, neste caso os empregadores, passaram a ser responsáveis pelo cumprimento do RGPD e, agora, da LPD, e têm de poder comprová-lo.

Ora, o empregador está sujeito a coimas de até 20.000.000€ ou 4% do volume de negócios anual, nos termos dos arts. 37.º e 38.º da LPD, se violar as obrigações previstas no RGPD.

Ademais, a LPD, nos arts. 46.º a 52.º, prevê crimes específicos em matéria de proteção de dados, como a utilização de dados de forma incompatível com a finalidade da recolha, o acesso indevido ou o desvio de dados.

As pessoas coletivas são responsáveis pelos crimes previstos na LPD, nos termos do art. 11.º do Código Penal.

Em face do exposto, entendemos que os empregadores podem implementar programas de compliance de proteção de dados desenhados à medida do nível de risco que os seus tratamentos de dados envolvem, com vista a (i) instituir uma cultura de proteção de dados e de privacidade em todos os níveis da organização, (ii) implementar os controlos adequados para prevenir e mitigar o risco da ocorrência de violações de dados e, por decorrência, da prática de contraordenações e de crimes à luz da LPD e (iii) atenuar ou mesmo excluir a responsabilidade dos empregadores por violações de dados ocorridas dentro da sua organização. ●