# A (R)EVOLUÇÃO NA REGULAÇÃO EUROPEIA SOBRE A PROTEÇÃO DE DADOS

***Inês Coelho Simões***

Se ouviu dizer que a sua empresa vai poder ser multada em mais de 20 milhões de euros pela má gestão dos dados pessoais dos seus trabalhadores, tem dois pontos a reter. O primeiro é simples: ouviu bem.

A culpa é do Regulamento (EU) 2016/679. Quatro anos volvidos desde o início das negociações, Parlamento, Conselho e Comissão chegaram a um entendimento que resultou em 173 "Considerandos" e 99 Artigos respeitantes à proteção, tratamento e circulação dos dados pessoais das pessoas singulares. A ideia foi uniformizar as diferentes legislações que existiam nos vários Estados-Membros, estabelecendo-se agora um conjunto de regras diretamente aplicáveis a cada um deles (e nem o "*Brexit*" abrirá exceção para o Reino Unido, no que concerne às relações comerciais ou serviços prestados aos restantes 27).

O segundo ponto a reter é o de que, e apesar de o Regulamento só entrar em vigor em 25 de maio de 2018, deve começar a preparar-se desde já. "Sem ter pressa, mas sem perder tempo" – gostando-se ou não deste Nobel – é, sem dúvida, o rumo a seguir.

É que, se em muito a Europa apenas repete ou concretiza direitos e deveres já consagrados na Diretiva de 95, certo é que, na maioria do texto comunitário, se introduzem alterações significativas que exigem das empresas uma preparação cuidada e uma revisão dos métodos de organização e proteção das informações constantes das suas bases de dados.

Organismos do Estado (com exceção dos Tribunais) e empresas cuja atividade principal implique o tratamento de dados sensíveis ou em grande escala têm, por enquanto, alguns deveres acrescidos: para elas é obrigatória a contratação de um "*Data Protection Officer*" ou "Encarregado da Proteção de Dados". Basicamente, trata-se de alguém que detenha conhecimentos sólidos sobre proteção de dados e a quem incumbirá, com independência, prestar aconselhamento e cooperar com as autoridades de controlo, em relação a quem atuará como ponto de contacto. O Regulamento prevê que este Encarregado possa ser um trabalhador da empresa ou um prestador de serviços – parece-nos, porém, que a independência exigida para o cargo se coaduna mais com a segunda; por outro lado, não sendo ainda obrigatória para todas as empresas parece-nos, também aqui, que o rumo mais provável a tomar pela U.E. será o da uniformização, pelo que as empresas poderão contratar desde já um Encarregado de Proteção de Dados (figura que, de resto, era já facultativa, antes da aprovação do Regulamento).

Sem prejuízo, qualquer que seja a estrutura, dimensão ou atividade da empresa/empregadora em causa, todas serão afetadas, a partir de 2018, por um conjunto de obrigações que, se não forem preparadas desde já, dificilmente poderão ser cumpridas, dada a complexidade das matérias e a exigência, sobretudo a nível tecnológico, que implica o seu acompanhamento. Será necessário, designadamente, rever os procedimentos respeitantes ao consentimento dos trabalhadores sobre o tratamento dos seus dados pessoais, aferir da necessidade de proceder a uma avaliação de impacto sobre os mesmos ("*privacy impact assessments*"), assegurar a efetividade do "esquecimento" a que os trabalhadores têm direito, proceder à "pseudonimização" e "cifragem" dos seus dados pessoais, rever a capacidade de "portabilidade" desses dados, e adotar diversos princípios de proteção de dados desde a conceção ("*privacy by design*") e por

defeito ("*privacy by default*") o mais cedo possível, adotando medidas que componham uma política interna efetiva de *compliance* de modo a assegurar a legalidade, neste novo quadro jurídico.

Podendo parecer, nalguns casos, excessivo, haverá que tomar consciência que direta ou indiretamente, conscientemente ou nem tanto, o volume de informação que as empresas atualmente detêm acerca dos trabalhadores assumiu uma dimensão sem precedente e é tanto mais detalhada quanto menos palpável se torna. As fichas A5 amarelas, ordenadas de A a Z, separadas por cartões e guardadas num armário são agora *megabytes*, arquivadas numa "nuvem" que requerem um controlo eficaz que, contudo, nem sempre se alcança: só depois de um anónimo exigir dinheiro pelo "resgate dos dados" é que o Banco Central Europeu deu conta da falta de endereços de email nas suas bases de dados, pirateadas em julho de 2014. Neste caso, 20 mil. Nos EUA, em julho do ano passado, *hackers* suspeitos de terem ligações ao Governo chinês acederam aos dados pessoais de 4 milhões de funcionários públicos. E ninguém sabe ainda a extensão (deste e de outros) *ciber*- desvios-de-informação.