(Ciber)segurança e privacidade: porque não podemos falar de uma sem a outra?

dinheirovivo.pt/opiniao/ciberseguranca-e-privacidade-porque-nao-podemos-falar-de-uma-sem-a-outra-12694668.html

29 de maio de 2020

A Cibersegurança e Privacidade estão, e estarão sempre, intrinsecamente ligadas. Por este motivo e uma vez que se assinala agora o 2º aniversário da implementação do RGPD (25 de maio), achei pertinente desmistificar a figura do Encarregado de Proteção de Dados (EPD), um verdadeiro pilar do RGPD que oferece enormes vantagens competitivas às empresas, em particular no plano da cibersegurança, bem como outros instrumentos que cruzam as referidas disciplinas, nomeadamente a garantia no cumprimento e conformidade legal decorrente do regulamento, e a evolução do nível de maturidade da organização no que respeita as boas práticas de segurança.

O EPD é a figura que faz a ponte entre privacidade e segurança.

Desde logo, deve reunir determinadas características profissionais bem como qualidades e conhecimentos especializados já que lhe cabe a difícil tarefa de informar e aconselhar a organização, mais especificamente a gestão de topo, no plano de fiscalização de implementação do RGPD e, ainda, cooperar com as autoridades, nomeadamente a própria Comissão Nacional de Proteção de Dados (CNPD), estando, ao mesmo tempo, vinculado à obrigação de sigilo ou de confidencialidade.

O EPD é hoje uma realidade presente nas entidades públicas, onde a sua designação é obrigatória, ainda que, nalguns setores, a sua implementação tenha sido extremamente difícil.

Importa, no entanto, ter presente que o EPD deve também ser uma realidade em entidades privadas com determinadas características, algo que tenho verificado que nem sempre acontece, o que pode ter consequências extremamente gravosas. Em causa estão todas as organizações com tratamento de dados em grande escala ou que tratem categorias especiais de dados - o que, convenhamos, é a realidade de muitas empresas do tecido empresarial português.

Da minha parte, e sabendo que a privacidade está na ordem do dia, seja pelos abusos e desrespeito que sofre, seja pelo aumento de ciberataques que a VisionWare tem vindo a denunciar e que, na sua maioria, resultam em enormes violações de dados, não posso deixar de recomendar que qualquer organização, mesmo que não esteja obrigada a designar um EPD, recorra, a título voluntário, a consultores externos com funções ligadas à proteção dos dados pessoais. Veja-se, a título de exemplo, a ocorrência de um incidente de segurança implicar a necessidade de comunicação ao Centro Nacional de Cibersegurança, mas também, à Comissão Nacional de Proteção de Dados (CNPD) sempre que implique uma violação de dados pessoais.

A verdade é que, seja com ou sem EPD, a implementação do RGPD é para cumprir.

Para isso, as empresas necessitam de rever minuciosamente e com a devida diligência as medidas técnicas/de segurança já existentes. As recomendações da Diretiva NIST, destinadas a garantir um elevado nível comum de segurança das redes e da informação, têm aqui um papel fundamental. Esta diretiva acaba por abranger as mesmas organizações que têm de designar um EPD, já que se dirige à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação.

É inegável que a especificidade das temáticas relativas à Cibersegurança implica uma abordagem dupla - tecnológica e jurídica -, mas, acima de tudo, trata-se de atingir um grau razoável de maturidade na dimensão de segurança e, assim, uma boa base de implementação do RGPD.

Bruno Castro é CEO da Visionware