29 de março de 2018

Magda Cocco | mpc@vda.pt
Inês Antas de Barros | iab@vda.pt
Maria de Lurdes Gonçalves | mlg@vda.pt

CIBERSEGURANÇA

REGIME JURÍDICO DA CIBERSEGURANÇA EM PORTUGAL – PROPOSTA DE LEI

Foi publicada, no dia 27 de março de 2018, a **Proposta de Lei n.º 119/XIII** que transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa às medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União ("Proposta de Lei").

Esta Proposta de Lei é aplicável: *(i)* à Administração Pública (incluindo a empresas públicas); *(ii)* aos operadores de infraestruturas críticas; *(iii)* aos operadores de serviços essenciais*; (iv)* aos prestadores de serviços digitais sob a jurisdição nacional (incluindo os serviços de mercado em linha – "online marketplaces", de motor de pesquisa e de computação em nuvem – "cloud computing"); e *(v)* a quaisquer entidades que utilizam redes e sistemas de informação.

Os operadores de serviços essenciais serão identificados pelo Centro Nacional de Cibersegurança até 9 de novembro de 2018, tendo por base a lista de sectores e subsectores elencados no anexo ao diploma e que abrange, entre outros, os seguintes sectores: bancário (instituições de crédito); energia (eletricidade, petróleo e gás); fornecimento e distribuição de água potável; infraestruturas digitais; infraestruturas do mercado financeiro; saúde (instalações de prestação de cuidados de saúde); transportes (aéreo, ferroviário, marítimo e por vias navegáveis interiores e rodoviário).

Esta Proposta de Lei estabelece: *(i)* a necessidade de uma Estratégia Nacional de Segurança do Ciberespaço a aprovar, por resolução do Conselho de Ministros e *(ii)* define a estrutura de "governança" da segurança do ciberespaço. Esta estrutura é composta pelo: Conselho Superior de Segurança do Ciberespaço (órgão específico de consulta do Primeiro-Ministro para assuntos relativos à segurança do ciberespaço), Centro Nacional de Cibersegurança (Autoridade Nacional de Cibersegurança) e "CERT.PT" (equipa de resposta a incidentes de segurança informática nacional, funcionando no Centro Nacional de Cibersegurança).

Adicionalmente, a Proposta de Lei determina que algumas entidades tenham de observar *(i)* determinados requisitos de segurança nas suas redes e sistemas de informação e *(ii)* notificar eventuais incidentes ao Centro Nacional de Cibersegurança (define-se "incidente" como um evento que tem um efeito adverso real na segurança das redes e dos sistemas de informação).

Prevê-se ainda a possibilidade de notificação voluntária de incidentes por parte das entidades não abrangidas pela obrigação legal.

Os requisitos de segurança e de notificação de incidentes serão detalhados, posteriormente, em legislação específica.

Fiscalização e coimas

As competências de fiscalização e de aplicação das sanções previstas na lei ficam a cargo do Centro Nacional de Cibersegurança. As infrações à lei podem determinar a aplicação de multas que variam, no caso das pessoas coletivas, entre € 2500 e € 5000, no caso de infrações muito graves, ou € 500 e € 1000, no caso de infrações graves.

A negligência será também punível, sendo nesse caso os limites mínimos e máximos das coimas reduzidos a metade.

Próximos passos

A Proposta de Lei seguiu no dia 28 de março para a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias e será, brevemente, discutida em Plenário, sendo importante acompanhar os seus desenvolvimentos.