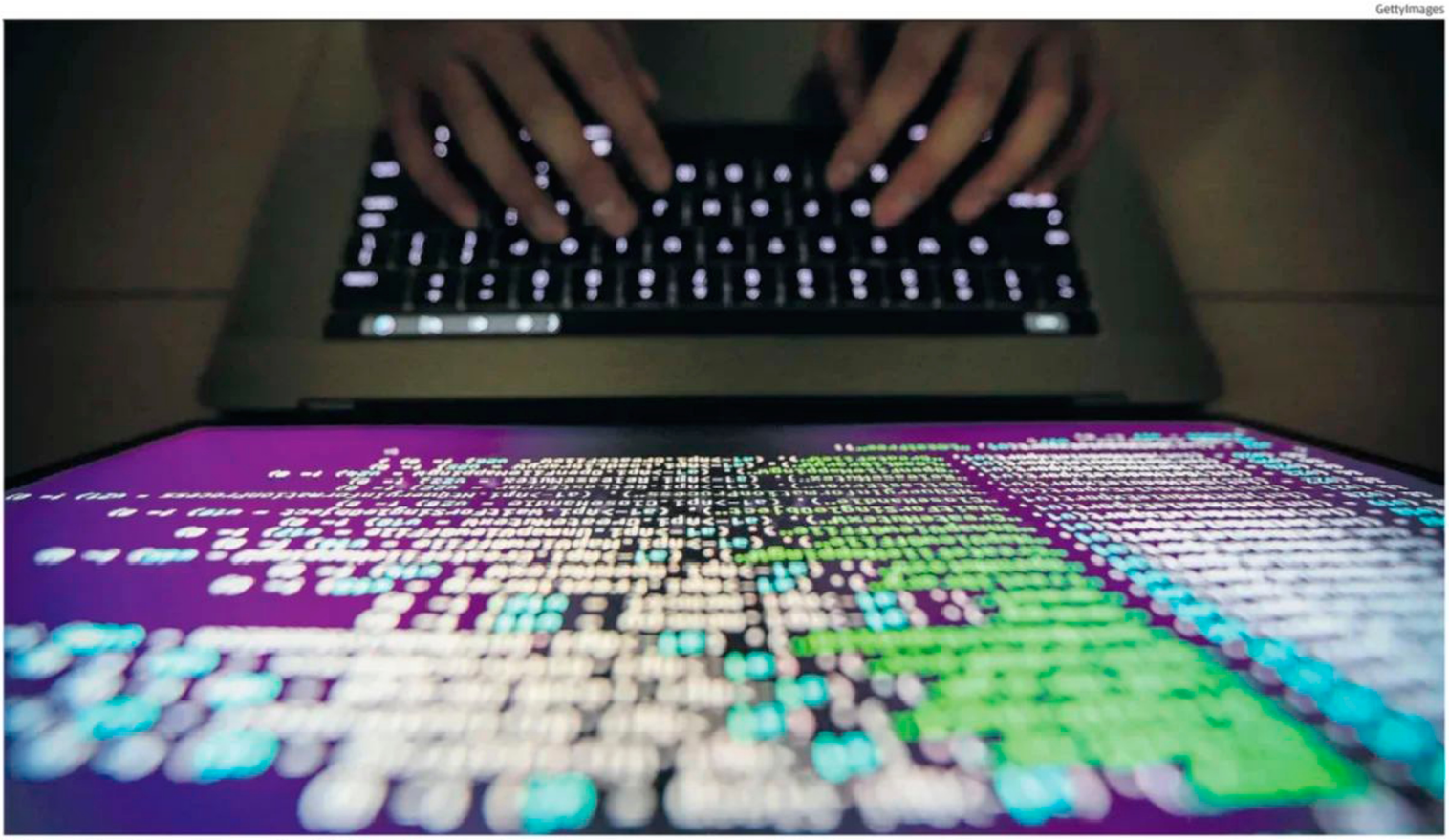
Jornal de Negócios
09.12.2024
P. 01

Gestores com multas pesadas se falharem na cibersegurança

Novo regime responsabiliza diretamente administradores e gerentes por falhas e aumenta em muito as coimas a aplicar. Leque de entidades abrangidas será alargado. ECONOMIA 10 e 11

GettyImages



Entidades abrangidas pelo novo regime terão 180 dias para se adaptarem.

REGULAMENTAÇÃO

Gestores com multas pesadas se falharem na cibersegurança

O novo Regime Jurídico da Cibersegurança vem responsabilizar diretamente os administradores e gestores por falhas e aumenta em muito as coimas a aplicar. O leque de entidades abrangidas será maior e abrange, de forma indireta, terceiros com quem colaborem, caso dos fornecedores.

FILOMENA LANÇA
filomenalanca@negocios.pt

Os titulares dos órgãos de administração, gestão e direção das entidades que, em matéria de cibersegurança, sejam consideradas "essenciais e importantes" serão responsáveis, por lei, por aprovar medidas de gestão de risco, por assegurar que estão implementadas e que há formação sobre elas. Em caso de incumprimento, se se comprovar que houve dolo ou culpa grave, terão de responder por isso e suportar o pagamento de coimas que podem atingir vários milhares de euros.

Esta é uma das novidades do novo Regime Jurídico da Cibersegurança, que transpõe uma diretiva comunitária, a chamada NIS2, e cuja proposta de lei, já aprovada em Conselho de Ministros, se encontra em consulta pública até 12 de dezembro, esperando-se que seja aprovada no Parlamento até ao final do ano. A entrada em vigor deverá acontecer 30 dias depois da publicação, mas a produção de efeitos, para a maioria das novas obrigações, só ocorre 18 meses depois, o que significa que as empresas - e o setor público, ao qual também se aplica – terão um prazo para se adaptarem. A nova lei, não só trará novas regras para a cibersegurança das organizações, como alarga o leque das entidades abrangidas por elas e que terão de investir nesta área.

A responsabilização dos dirigentes, com a possibilidade de poderem ter de "responder diretamente por qualquer infração cometida nos termos deste diploma é uma das grandes alterações da NIS2", explica Inês An-

> **[A ideia é] conseguir um maior incentivo à aplicação da lei, ficando esse ónus do lado dos administradores.**
> **RICARDO HENRIQUES**
> Abreu Advogados

tas de Barros, advogada e especialista em cibersegurança da VdA. A ideia é "conseguir um maior incentivo à aplicação da lei, ficando esse ónus do lado dos administradores", acrescenta Ricardo Henriques, da Abreu.

Basicamente, caberá aos administradores "fazer todo o acompanhamento e garantir que a entidade cumpre com as suas obrigações e regras", sendo que "não será uma falha de detalhe ou de pormenor que os vai responsabilizar", acrescenta o especialista. Mas se atuar com dolo implica uma intenção clara de cometer um ilícito, a culpa grave "é equivalente à negligência grosseira", o que acontecerá "nas situações mais graves em que o administrador ou não verificou o cumprimento das regras ou fê-lo de forma pouco cuidada, face ao que lhe seria exigível".

E de que sanções estamos a falar? O diploma prevê, para as pessoas singulares, coimas que, dependendo do incumprimento em causa, começam nos 250 euros, mas podem chegar aos 250 mil. Para as pessoas coletivas chegam a atingir os dez milhões de euros ou o equivalente a 2% do volume de negócios anual a nível mundial, consoante o que for mais elevado. E a estas coimas podem somar-se ainda sanções acessórias, como a proibição de participar em contratação pública ou a suspensão da prestação do serviço enquanto não estiverem com tudo em ordem, ainda, multas diárias por atraso no cumprimento. "Até agora o quadro sancionatório não era muito pesado, o que demovia as entidades de colocarem isto no topo das suas prioridades, quando o que se quer é que a cibersegurança esteja no ADN das organizações", acrescenta Inês Antas de Barros.

Mais entidades abrangidas

As novas regras vão aplicar-se ao setor privado e ao público e as várias entidades serão divididas entre "importantes" e "essenciais", elencando um conjunto de critérios para determinar os setores cobertos e, dentro destes, as empresas abrangidas (volume de negócios ou número de trabalhadores, por exemplo). "Há um reforço claro dos setores considerados essenciais para a economia" e que passam a ter de cumprir todo um conjunto de regras em matéria de cibersegurança, nomeadamente de gestão de riscos", diz Inês Antas de Barros.

E setores em que um potencial ataque tenha grande impacto para a sociedade estão todos abrangidos. Comunicações, energia, transportes, saúde, águas, são todos essenciais e, dentro deles, as empresas que aí atuam têm todas as hipóteses de também ser. Com a nova lei entram aqui, por exemplo, os serviços postais; as entidades que realizam atividades de investigação e desenvolvimento de medicamentos; ou o setor do hidrogénio, elenca a especialista.

O Quadro Nacional de Referência para a Cibersegurança vai ser revisto e, com base nele, as entidades terão de adotar um quadro de gestão de risco, identificando a sua própria realidade e adequando as respostas necessárias à luz do que a lei prevê.

Uma outra novidade, explica Inês Antas de Barros, é o foco na segurança da cadeia de abastecimento, "porque se percebeu que, muitas vezes, os riscos estão nos terceiros, nos prestadores de serviços, nos fornecedores". Assim, "há um reforço do dever de diligência na escolha de um terceiro, avaliando se ele oferece as mesmas garantias que a organização tem também implementadas e indo monitorizando". E isso, desde logo, nos próprios contratos, para "responsabilizar ao máximo em caso de incidentes". Ao mesmo tempo, acrescenta Ricardo Henriques. "Isto acabará por ter um efeito ao nível das entidades abrangidas, alargando o leque, ainda que de forma indireta".

A competência para fiscalizar o cumprimento da lei mantém-se no Centro Nacional de Cibersegurança - juntamente com algumas entidades setoriais de supervisão - o qual ganha poderes acrescidos de fiscalização e auditoria e será quem vai sancionar em caso de incumprimento. ■

A nova lei traz novas regras e alarga o leque das entidades abrangidas que terão de investir em cibersegurança.

PERGUNTAS A INÊS ANTAS DE BARROS
Especialista da VdA

"Há muitas empresas a começar do zero"

Como é que as empresas vão olhar para estas novas regras e lidar com elas? Já estão a fazê-lo?
Temos realidades muito distintas no tecido empresarial português, que é constituído sobretudo por PME. E, apesar de algumas destas poderem até ser excluídas do âmbito da aplicação, pela sua dimensão, também há muitas empresas que não são PME e que estão cobertas, mas que o nível de maturidade é muito inferior. Há empresas e há setores que já estavam cobertos pela anterior diretiva e onde este tema já está na agenda, muitas vezes porque já sofreram ataques, e, portanto, têm um nível de maturidade superior e, aí, eventualmente, o caminho será menos difícil. Não vai ser fácil, vai ser menos difícil. Para outras, muitas, estamos a começar do zero. Não é por acaso que o legislador dá 18 meses para implementar.

Esses 18 meses serão suficientes? E se não cumprirem?
Não são. Teoricamente, após os 18 meses, a autoridade pode começar a sancionar. Eu acho que a autoridade, o Centro Nacional de Cibersegurança, vai adotar uma postura muito pedagógica nos tempos iniciais. Isso seria essencial para permitir às organizações implementar e perceber o que é que têm e não têm que fazer.

E o que é que cada empresa tem de fazer?
Tem de olhar para os requisitos que se aplicam à organização, perceber o que tem dentro da casa e identificar os 'gaps'. Para depois ter um plano de ação, com um calendário, e perceber que medidas vai adotar. Cibersegurança é caro. Muitas vezes implica a adoção de ferramentas tecnológicas que são caras. E que implicam um grande investimento. Portanto, nós estamos agora numa altura ideal nas organizações que estão a preparar o orçamento do próximo ano, as que já estejam cobertas, já a calendarizar e programar estes investimentos.

Eu acho que a autoridade, o Centro Nacional de Cibersegurança, vai adotar uma postura muito pedagógica nos tempos iniciais.

Como é que uma empresa sabe que está coberta?
A lei tem uma listagem dos setores. Mas não é uma evidência, porque aquilo depois é um puzzle, há vários critérios a considerar, mas esse é o primeiro passo, perceber se é uma entidade importante, ou essencial, ou então uma entidade pública, relevante de grupo A ou grupo B. Analisado o perímetro, tem de identificar os requisitos que lhes são aplicados. Esse é o ponto de partida. E isso devia ser feito ontem.

Pode dizer-se que a generalidade das nossas PME estão obrigadas?
Sem distinguir entre PME e grandes empresas, eu diria que a maior parte ou a grande parte do tecido empresarial ou das entidades estarão cobertas.

Mesmo as mais pequenas?
Depende do setor. E mesmo que eu seja uma pequena empresa, se for, suponhamos, a única empresa naquele setor ou que tenha uma quota de mercado considerável, então passa a estar coberta.

O público estará mais bem preparado do que o privado?
Olhando para casos tornados públicos nos últimos tempos, diria que há muitas entidades do setor público que têm um grande caminho pela frente.

Recentemente a AMA teve um ataque grave.
Exatamente. E a AMA até tem este sistema muito trabalhado, com muitas ferramentas tecnológicas. A grande maioria das entidades públicas tem um grande volume de informação, muito mais do que algumas do privado. E como são atividades essenciais para a sociedade têm um risco superior. E são logo identificadas como de risco mais elevado. Portanto, eu diria que o setor público tem um grande caminho pela frente para se tornar mais resiliente e gerir de forma mais eficiente os riscos de cibersegurança. Mas o privado também. ■