

LEGAL ALERT

REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

Entrou em vigor esta semana a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016.

O objetivo deste regime é garantir um elevado nível comum de segurança das redes e dos sistemas informáticos em toda a União Europeia, impondo deveres a várias entidades especialmente suscetíveis de sofrerem incidentes de segurança com repercussões graves.

As entidades abrangidas por este regime incluem:

- i)* **Administração Pública:** Estado, regiões autónomas, autarquias locais, entidades administrativas independentes, institutos públicos, empresas públicas e associações públicas;
- ii)* **Operadores de infraestruturas críticas:** entidades que operem uma componente ou sistema essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;
- iii)* **Prestadores de serviços essenciais:** entidades que prestem serviços nos setores da eletricidade, do petróleo, do gás, dos transportes (aéreo, ferroviário, marítimo e rodoviário), das instituições de crédito, dos operadores de plataformas de negociação e contrapartes centrais, da prestação de cuidados de saúde, do fornecimento e distribuição de água potável ou das infraestruturas digitais, especificamente dos serviços de pontos de troca de tráfego, serviços de *Domain Name System* e de registo de nomes de domínio de topo;
- iv)* **Prestadores de serviços digitais:** entidades que prestem serviços de mercado em linha (*online marketplaces*), de motor de pesquisa em linha (*online search engines*) ou de computação em nuvem (*cloud computing*).

Os deveres das entidades abrangidas pelo regime jurídico em causa incluem:

- i)* Dever de cumprir os requisitos de segurança estabelecidos na lei;
- ii)* Dever de notificar o Centro Nacional de Cibersegurança sempre que sejam detetados incidentes com um impacto relevante ou substancial na segurança das redes ou sistemas de informação ou na prestação dos serviços;
- iii)* Dever de comunicar ao Centro Nacional de Cibersegurança o exercício da atividade de prestador de serviços essenciais no setor das infraestruturas digitais e do exercício da atividade de prestador de serviços digitais.

Os requisitos de segurança e de notificação, com exceção dos requisitos de segurança aplicáveis aos prestadores de serviços digitais, deverão ser definidos em legislação própria, que deverá ser aprovada no prazo de 150 dias após a entrada em vigor do presente regime jurídico. Nesta medida, **atualmente, apenas os prestadores de serviços digitais se encontram obrigados a cumprir os requisitos de segurança.**

Os requisitos de segurança a cumprir pelos prestadores de serviços digitais implicam a identificação e a adoção de medidas técnicas e organizativas adequadas e proporcionais aos riscos que se colocam à segurança das redes e dos sistemas de informação, tendo em conta os **progressos técnicos mais recentes** e os seguintes fatores:

- i)* Segurança dos sistemas e das instalações;
- ii)* Tratamento dos incidentes;
- iii)* Gestão da continuidade das atividades;
- iv)* Acompanhamento, auditoria e testes realizados; e
- v)* Conformidade com especificações técnicas internacionais.

Os requisitos de segurança e de notificação de incidentes **não são aplicáveis a:**

- i)* **Micro ou pequenas empresas:** empresas com menos de 50 trabalhadores e cujo volume de negócios anual ou balanço total anual não exceda os 2 000 000,00 EUR;
- ii)* **Empresas de comunicações eletrónicas:** empresas que ofereçam redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, que já estejam sujeitas às obrigações dos artigos 54.º-A a 54.º-G da Lei n.º 5/2004, de 10 de fevereiro (Lei das Comunicações Eletrónicas);

iii) **Prestadores de serviços de confiança:** empresas que ofereçam serviços de criação, verificação e validação de assinaturas e selos eletrónicos e autenticação de websites.

Os prestadores de serviços essenciais do setor das infraestruturas digitais e os prestadores de serviços digitais, com exceção das micro e pequenas empresas, **devem comunicar de imediato ao Centro Nacional de Cibersegurança o exercício da respetiva atividade.**

As infrações aos deveres previstos no regime jurídico da segurança do ciberespaço constituem contraordenações.

O incumprimento da obrigação de implementar os requisitos de segurança previstos para os prestadores de serviços digitais consubstancia uma **contraordenação muito grave**, punida com uma coima de 5 000,00 EUR a 25 000,00 EUR, tratando-se de pessoa singular, e de 10 000,00 EUR a 50 000,00 EUR, tratando-se de pessoa coletiva.

O incumprimento da obrigação de notificação do exercício de atividade no setor das infraestruturas digitais ou da obrigação de identificação como prestador de serviços digitais consubstancia uma **contraordenação grave**, punida com uma coima de 1 000,00EUR a 3 000,00 EUR, tratando-se de pessoa singular, e de 3 000,00 EUR a 9 000,00 EUR, tratando-se de pessoa coletiva.

Os quadros legais da proteção da informação encontram-se num processo de profunda transformação, gerando crescentes desafios para as empresas. Na MLGTS, trabalhamos para tornar o cumprimento da legislação aplicável mais acessível e com o menor impacto possível nas respetivas atividades.

Tiago Félix da Costa [+info]
Frederico Machado Simões [+info]