CIBERSEGURANÇA E COMBATE A CONTEÚDOS TERRORISTAS ONLINE

SUMMARY

O Governo recebeu autorização para legislar sobre o quadro legal da segurança digital:

- *Implementando a Diretiva SRI 2 com um novo regime jurídico da cibersegurança e com mais obrigações de gestão e notificação de riscos a entidades públicas e privadas.*
- *Criando os mecanismos nacionais para a remoção e bloqueio de conteúdos terroristas online.*

CONTACTOS

JOÃO MACEDO VITORINO

JVITORINO@MACEDOVITORINO.COM

PEDRO RAMALHO DE ALMEIDA

PALMEIDA@MACEDOVITORINO.COM

BERNARDO SANTANA

BSANTANA@MACEDOVITORINO.COM

Duas leis publicadas em Diário da República, autorizam o Governo a atualizar o quadro legal nacional em matéria de segurança digital.

A Lei n.º 59/2025 autoriza o Governo a aprovar o regime jurídico da cibersegurança, transpondo a Diretiva (UE) n.º 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, também designada Diretiva SRI 2, destinada a garantir um nível comum de cibersegurança em toda a União. São as seguintes as principais novidades:

- Extensão do âmbito de aplicação do regime de cibersegurança a uma parte substancial da Administração Pública e às entidades classificadas como essenciais, importantes e públicas relevantes, embora exclua as entidades dos domínios da segurança nacional, segurança pública, defesa e informações. A qualificação destas entidades assenta em critérios como a importância da atividade, a exposição a riscos e a gravidade potencial dos incidentes. As organizações devem, por isso, começar a identificar a sua provável categoria para antecipar as obrigações que lhes serão aplicáveis.
- A Estratégia Nacional de Segurança do Ciberespaço, que definirá as prioridades e os objetivos estratégicos nacionais em matéria de cibersegurança;
- O Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança em grande escala, que regulará e aperfeiçoará a gestão deste tipo de incidentes; O Quadro Nacional de Referência para a Cibersegurança, que reunirá e divulgará as normas, padrões e boas práticas aplicáveis à gestão da cibersegurança.
- A criação de um novo Conselho Superior de Segurança do Ciberespaço, como órgão consultivo do Primeiro-Ministro; do Centro Nacional de Cibersegurança, como autoridade nacional de cibersegurança; e do Gabinete Nacional de Segurança e a Autoridade Nacional de Comunicações, como autoridades setoriais; e a Autoridade de Supervisão de Seguros e Fundos de Pensões, a Comissão do Mercado de Valores Mobiliários e o Banco de Portugal, como autoridades nacionais especiais de cibersegurança.

- O Centro Nacional de Cibersegurança terá competência para supervisionar o cumprimento das obrigações através de inspeções, auditorias, verificações, pedidos de informação e emissão de instruções vinculativas. Poderá ainda suspender certificações, autorizações ou licenças e determinar o bloqueio ou redirecionamento de endereços IP.
- Obrigações específicas aos órgãos de gestão e administração das entidades abrangidas, incluindo a implementação de um sistema de gestão de riscos de cibersegurança. Prevê-se ainda a realização de análises de risco residual, a elaboração de relatórios anuais e a designação de um responsável de cibersegurança. As entidades terão ainda de notificar à autoridade competente qualquer incidente significativo nesta matéria.
- Um regime contraordenacional em matéria de cibersegurança. As entidades poderão solicitar fundamentadamente à autoridade de cibersegurança competente a dispensa da aplicação de coimas durante os primeiros 12 meses de vigência do regime.
- A criação de um gabinete de crise para a coordenação de incidentes com impacto na segurança interna e a revisão da Lei do Cibercrime, despenalizando, em determinadas condições, condutas destinadas à identificação de vulnerabilidades, desde que sem finalidade de obtenção de vantagem económica e com comunicação imediata ao responsável pelo sistema.
- A Lei n.º 60/2025 adapta a ordem jurídica interna ao Regulamento (UE) n.º 2021/784, relativo à prevenção e combate à difusão de conteúdos terroristas online. Destacamos os seguintes pontos do seu conteúdo:
- A Polícia Judiciária é designada como a autoridade competente para emitir decisões de supressão ou bloqueio de conteúdos terroristas, comunicando-as de imediato ao Ministério Público junto do DCIAP e remetendo o respetivo relatório. No prazo máximo de 48 horas, o Ministério Público deve apresentar a decisão ao juiz de instrução para validação, sob pena de caducidade.
- O novo regime de recursos prevê que das decisões do juiz de instrução cabe recurso para o Tribunal da Relação, sendo partes legítimas os prestadores de serviços de alojamento virtual, os fornecedores de conteúdos e os representantes legais de prestadores sem estabelecimento principal na União Europeia.
- Em matéria contraordenacional, o diploma determina que o incumprimento do Regulamento constitui infração punível com coima, sendo competente para apreciar os respetivos recursos o Tribunal da Concorrência, Regulação e Supervisão.
- O regime quadro das contraordenações do setor das comunicações é igualmente alargado, passando a abranger estas infrações. Os juízos de pequena criminalidade ficam responsáveis por decidir os recursos das decisões das autoridades administrativas previstas no Regulamento.

As autorizações legislativas têm a duração de 180 dias. As organizações devem desde já avaliar o impacto das alterações, com vista a assegurar uma adaptação célere quando forem aprovados os decretos-lei de execução.