



Nota Informativa

Recomendação (UE) n.º 2019/533 da Comissão de 3 de abril de 2019, sobre a cibersegurança no sector da energia

No dia 05 de abril, foi publicada no Jornal Oficial da União Europeia (“JOUE”) a Recomendação (UE) n.º 2019/533 da Comissão de 3 de abril de 2019, sobre a cibersegurança no sector da energia.

A referida Recomendação surge atendendo a que o “*âmbito da transição energética e da concomitante descentralização da produção de energia a partir de fontes renováveis, o progresso tecnológico, o acoplamento de setores e a digitalização [que] estão a transformar a rede elétrica da Europa numa «rede inteligente»*” (cfr. considerando 1 da Recomendação).

Sendo que esta nova realidade acarreta “*novos riscos, dado que a digitalização expõe cada vez mais o sistema energético a ataques informáticos e a incidentes que podem comprometer a segurança do aprovisionamento energético*” (cfr. considerando 1 da Recomendação).

A presente recomendação vem, assim, identificar as principais questões relacionadas com a cibersegurança no setor da energia, tendo como destinatários os Estados-Membros e os operadores de rede de energia.



Nestes termos, dispõe a presente recomendação que os Estados-Membros devem *“incentivar as partes interessadas a adquirirem competências e conhecimentos relacionados com a cibersegurança no setor da energia, incluindo, estas considerações no seu quadro nacional através de estratégias, leis, regulamentos e outras disposições administrativas”* (cfr. n.º 2 da Recomendação).

Nesse sentido, a Recomendação vem determinar quais os requisitos em tempo real das componentes da infraestrutura energética que devem ser preenchidos, tanto pelos Estados-Membros, como pelos operadores de rede de energia, uma vez que alguns elementos do sistema energético têm de funcionar em tempo real, ou seja, reagir a comandos em poucos milissegundos, o que torna difícil ou mesmo impossível aplicar medidas de cibersegurança, por falta de tempo. (cfr. n.º 3 da Recomendação).

Nos termos da Recomendação em causa, os Estados-Membros devem assegurar que as partes interessadas, nomeadamente os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI, aplicam as medidas em matéria de cibersegurança, relacionadas com os efeitos em cascata no setor da energia, atendendo que as redes de eletricidade e os gasodutos estão fortemente interligados em toda a Europa. (cfr. n.º 6 da Recomendação).

Por esta razão, recomenda-se que os Estados-Membros procedam a uma avaliação das interdependências e se assegurem que os operadores de rede dispõem de um *“quadro de comunicação com todas as principais partes interessadas, para partilhar os sinais de alerta precoce e cooperar em matéria de gestão de crises”*. (cfr. n.º 7 da Recomendação).



Já quanto aos operadores da rede, a recomendação fixa que, em especial, devem *“garantir que os novos dispositivos (nomeadamente no âmbito da «Internet das coisas») têm e mantêm um nível de cibersegurança adequado à importância crítica do local”* e que *“ponderem devidamente os efeitos ciberfísicos ao estabelecerem e reverem periodicamente os planos de continuidade das atividades; estabelecer critérios de conceção e uma arquitetura para uma rede resiliente.”* (cfr. ponto 8 da Recomendação)

Em relação à combinação das tecnologias antigas e de ponta, a Recomendação encarrega os Estados-Membros de *“assegurar que as partes interessadas, aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com a combinação de tecnologias clássicas e de ponta no setor da energia.”*, *“incentivar os operadores de redes de energia e os fornecedores de tecnologia a adotarem, sempre que possível, as normas internacionalmente aceites em matéria de cibersegurança”* (cfr. ponto 9 da Recomendação).

Quanto aos operadores de redes de energia, a recomendação elenca vários deveres, entre eles, destaque-se o dever de *“analisar os riscos inerentes à ligação de dispositivos clássicos e do domínio da «Internet das coisas» e ter conhecimento das interfaces internas e externas e das suas vulnerabilidades”* e o de *“tomar medidas adequadas contra-ataques malévolos provenientes de um grande número de aplicações ou dispositivos de consumo que possam ser controlados por entidades mal-intencionadas”* (cfr. ponto 12 da Recomendação).

Por fim, a Recomendação encarrega os Estados- Membros de transmitir à Comissão, 12 meses após a sua publicação, e posteriormente, de 2 em 2 anos, informações pormenorizadas sobre o estado de execução da recomendação, através do grupo de cooperação SRL. Sendo que, *“com base nas informações apresentadas pelos Estados-Membros, a Comissão analisará a aplicação da presente recomendação e avaliará a*



TELLES GREEN BRIEFING



Área de prática de Ambiente,
Energia e Recursos Naturais

eventual necessidade de adotar novas medidas, após consulta dos Estados-Membros e das partes interessadas pertinentes” (cfr. ponto 13 da Recomendação).

Para mais informações,

Ivone Rocha

[\(i.rocha@telles.pt\)](mailto:i.rocha@telles.pt)

AMBIENTE, ENERGIA E RECURSOS NATURAIS

A Área de Prática de Ambiente, Energia e Recursos Naturais, da TELLES, conta com uma equipa com especializações em Direito Público/Administrativo e Direito do Ambiente, com Mestrados e Pós-Graduações realizadas nessas áreas jurídicas e larga experiência profissional nestes sectores, inserida num quadro de multidisciplinidade com uma abordagem jurídica inovadora do ambiente e da energia.

