Bom dia,

Bem-vindo(a) à newsletter #122 da DPO Consulting, o nosso meio informativo sobre o mundo da Privacidade, Proteção de Dados, *Compliance* e Inteligência Artificial.

Contacte-nos e leve a sua conformidade a outro nível.

Proteja os Dados. Reforce a Confiança. Simplifique a Conformidade.

Digital Omnibus: quando simplificar significa desproteger

O ECO publicou, dia 4 de março, o artigo de opinião de Elsa Veloso onde a nossa CEO analisa de forma crítica a proposta Digital Omnibus da Comissão Europeia e os seus potenciais efeitos sobre o quadro regulatório digital europeu.

A iniciativa tem como propósito aliviar algumas obrigações regulatórias no domínio digital, reduzindo encargos administrativos e reforçando a competitividade das empresas europeias. Mas a simplificação normativa abre um debate que não pode ser ignorado: até onde pode ir a redução de exigências sem comprometer mecanismos essenciais de proteção, nomeadamente no que respeita aos direitos digitais, à proteção de dados e à responsabilidade das plataformas?

Para Elsa Veloso, a resposta é clara: simplificar não pode significar, diluir nem desproteger. As salvaguardas que sustentam a confiança no ecossistema digital não são burocracia dispensável, são a base sobre a qual assenta a relação entre cidadãos, empresas e plataformas. O equilíbrio entre competitividade económica e proteção de direitos fundamentais permanece um dos desafios mais exigentes da governação digital na União Europeia.

Este debate ganha ainda maior acuidade num contexto em que instrumentos como o AI Act, o Regulamento dos Serviços Digitais e outras iniciativas europeias estão ainda em fase de consolidação. Qualquer processo de simplificação que enfraqueça os princípios de responsabilidade, transparência e controlo do risco arrisca comprometer anos de construção regulatória.

Leia aqui o artigo completo

Autoridade italiana trava Amazon: recolha de dados de saúde e atividade sindical de trabalhadores considerada ilegal

A autoridade italiana de proteção de dados, o **Garante per la Protezione dei Dati Personali**, ordenou à **Amazon** a cessação imediata da recolha e

tratamento de dados sensíveis de trabalhadores num centro logístico situado nos arredores de Roma. A investigação concluiu que a empresa estava a recolher e a partilhar com gestores informação claramente para além do necessário para a gestão da relação laboral.

Segundo o regulador, eram tratados dados particularmente delicados, incluindo informações sobre condições de saúde, filiação ou participação sindical, envolvimento em greves e aspetos da vida familiar dos trabalhadores. Em vários casos, esses dados eram conservados durante anos e integrados em sistemas internos de monitorização, prática considerada incompatível com os princípios do **Regulamento Geral sobre a Proteção de Dados**.

A decisão identificou ainda práticas de vigilância consideradas desproporcionais, nomeadamente a instalação de câmaras de videovigilância em zonas adjacentes a áreas de descanso e instalações sanitárias. Para o regulador italiano, o caso ilustra os riscos crescentes da monitorização algorítmica em ambientes de trabalho altamente digitalizados e reforça uma mensagem clara para as organizações: tecnologias de vigilância laboral exigem avaliações rigorosas de proporcionalidade e modelos robustos de *workplace data governance*.

Saiba mais

Bruxelas endurece regras de cibersegurança: NIS2 e CSA2 entram numa nova fase

A 20 de janeiro de 2026, a **Comissão Europeia** apresentou um novo pacote legislativo que reformula a política europeia de cibersegurança, combinando uma revisão profunda do **Cybersecurity Act** (CSA2) com alterações dirigidas à **Diretiva NIS2**. O objetivo é reforçar a resiliência digital da União, reduzir a fragmentação regulatória e responder de forma mais eficaz aos riscos

emergentes nas cadeias de abastecimento de tecnologias de informação e comunicação.

No caso da NIS2, as propostas concentram-se na clarificação do âmbito de aplicação e na harmonização entre Estados-Membros. Passam a abranger novos atores, como fornecedores das futuras European Business Wallets e operadores de infraestruturas estratégicas de dupla utilização, ao mesmo tempo que alargam às empresas não europeias que prestam serviços na UE a obrigação de designar um representante no território europeu. Entre as novidades técnicas, destaca-se a integração da criptografia pós-quântica no planeamento nacional de cibersegurança, com metas de transição fixadas para 2030 nos casos críticos e 2035 nos restantes.

Já a reforma do CSA2 introduz mudanças estruturais: a certificação europeia de cibersegurança deixa de ser apenas um selo voluntário de qualidade para se tornar um instrumento central de acesso ao mercado. O papel da **ENISA** é reforçado e surge um novo quadro europeu para cadeias de abastecimento de TIC de confiança, permitindo identificar fornecedores de alto risco e impor medidas vinculativas, incluindo restrições ao uso de determinados componentes. Em paralelo, o pacote Digital Omnibus propõe um ponto único de notificação de incidentes e violações de dados, com prazo de reporte alargado para 96 horas. As negociações já começaram e o acordo político é esperado para 2027 - um sinal claro de que a cibersegurança passou definitivamente do domínio técnico para o centro da *governace* corporativa e da gestão de risco.

Leia a notícia na íntegra

Sines na corrida europeia da IA: Portugal e Espanha lançam gigafábrica de €8 mil milhões

Portugal e Espanha avançaram com uma candidatura conjunta para instalar uma Gigafábrica Europeia de Inteligência Artificial, num projeto paritário anunciado no âmbito da Cimeira Ibérica e avaliado em cerca de 8 mil milhões de euros. Do lado português, Sines foi escolhida para acolher parte da infraestrutura, beneficiando da sua posição estratégica como hub de conectividade internacional, graças aos cabos submarinos que ligam a Europa às Américas.

A futura infraestrutura deverá atingir uma capacidade próxima dos 150 megawatts de computação, suportada por mais de 100 mil GPUs de última geração, permitindo fornecer serviços avançados de IA a empresas, universidades, centros de investigação e entidades públicas. A **NVIDIA** participa como parceira tecnológica do projeto, reforçando a ambição de posicionar a Península Ibérica como um novo polo europeu de computação avançada.

O modelo financeiro prevê uma contribuição inicial de 6 milhões de euros por parte de cada país, com financiamento adicional da **União Europeia** e investimento empresarial apoiado pelo Banco Português de Fomento. Integrada na estratégia europeia de "soberania aberta", a iniciativa procura reduzir a dependência tecnológica externa e desenvolver infraestrutura crítica de IA. A dimensão do projeto levanta, contudo, desafios relevantes em matéria de governança de dados, cibersegurança e conformidade com o AI Act, aspetos que terão de ser incorporados desde a conceção da operação.

Leia a notícia na íntegra

Quando a Inteligência Artificial decide: quem assume a responsabilidade?

Num artigo publicado a 6 de março na Líder Magazine, Elsa Veloso coloca o dedo numa das questões mais prementes da adoção de Inteligência Artificial nas organizações: quando um sistema automatizado toma, ou influencia, uma decisão, quem é responsável pelo resultado?

À medida que a IA ganha terreno nos processos internos e nas escolhas estratégicas, a resposta a esta pergunta deixou de ser opcional. Torna-se imperativo definir mecanismos claros de supervisão humana e estruturas sólidas de governance que acompanhem, em tempo real, o que os sistemas fazem e porquê.

A automatização não dilui a responsabilidade, transfere-a e, em muitos casos, amplifica-a. Saber quem decide, quem supervisiona e quem responde pelos resultados gerados pela IA é hoje uma exigência de gestão tão crítica como qualquer outra decisão de negócio.

Com a entrada em vigor do AI Act, este imperativo ganha força regulatória. As organizações são chamadas a demonstrar controlo efetivo sobre os sistemas que utilizam, com transparência, gestão de risco e uma cultura de *accountability* que não começa na tecnologia, mas nas pessoas que a governam.

Leia o artigo

Partilhe, querendo, a newsletter da DPO Consulting.

Ficamos ao dispor para qualquer esclarecimento que haja por conveniente e voltamos ao contacto na próxima newsletter, com mais novidades e informações de relevo.

Até breve.
Elsa Veloso
CEO da DPO Consulting

DPO Consulting
Avenida da República, nº 18 3º - 1050-191 Lisboa
Rua Eugénio de Castro, 370 – H185 4100-225 Porto