Reconhecimento da cooperação europeia na Proteção de Dados e Cibersegurança

eco.sapo.pt/opiniao/reconhecimento-da-cooperacao-europeia-na-protecao-de-dados-e-ciberseguranca

22 de dezembro de 2022

O EDPS e a ENISA comprometem-se a apresentar um plano estratégico para a capacitação e consciencialização das diferentes instituições da União Europeia.

No passado dia 30 de novembro, a Autoridade Europeia para a Proteção de Dados (AEPD/EDPS) e a Agência da União Europeia para a Cibersegurança (ENISA) foram signatárias de um assinalável *memorandum* de entendimento que pretende garantir os direitos fundamentais dos utilizadores, em termos de segurança e proteção de dados, na utilização da Internet. Este *memorandum* assinala o esforço institucional por parte das Autoridades Europeias na definição de um quadro legal para a União que seja robusto o suficiente para mitigar os riscos inerentes à evolução tecnológica da década digital, de forma a garantir que o recurso global e aberto à Internet seja realizado em pleno respeito pelos direitos fundamentais dos seus utilizadores, reforçando a segurança e garantindo a proteção de dados.

Na senda da estratégia de cibersegurança da União para a década digital, emanada em conjunto pelo Parlamento e Conselho Europeus, do qual nascem as Directivas NIS e NIS 2.0, as duas entidades a **AEPD/EDPS** – autoridade de supervisão independente responsável por assegurar que os direitos à privacidade e proteção de dados são respeitado pelas instituições e órgãos da União Europeia, e a **ENISA** – agência da União, dedicada à aquisição de um nível mais elevado comum de cibersegurança, em toda a Europa – reconhecendo interesses comuns, firmaram a sua cooperação estratégica e a intenção de definir, estabelecer, e promover um quadro comum de atuação para as áreas da cibersegurança e proteção de dados, que vigorará nos próximos 5 anos.

A NIS 2.0 alarga o âmbito de um conjunto de obrigações relacionadas com a diligência da cadeia de fornecimento/abastecimento, exigindo que as entidades implementem **medidas de gestão do risco cibernético**, que incluem **requisitos de mitigação do risco de segurança** e **due diligence de terceiros,** aplicável aos setores e entidades já referenciados pela NIS: operadores de serviços essenciais, infraestruturas críticas e administração pública, porém, agora deixando margem aos Estados-Membros para que incluam no âmbito destas obrigações, as entidades que possam ser consideradas importantes no seu país.

Aquela cooperação, fazia já parte das intenções anunciadas na estratégia da **AEPD/EDPS** para 2020-2024, com a finalidade de contribuir para a conformação de um futuro digital mais seguro; o entendimento assenta, essencialmente na concordância em apresentar um plano estratégico para promover a sensibilização, ciberhigiene, privacidade

e proteção de dados nas Instituições, Agências e Órgãos da União, bem como à adoção de tecnologias que melhorem a privacidade dos titulares dos dados e fortaleçam as capacidades daquelas instituições.

Como demonstração do compromisso, declararam a pretensão de reunir-se, pelo menos, uma vez por ano, para analisar questões tais como: o plano estratégico, identificar outras áreas de cooperação, trocar pontos de vista sobre os principais desafios atuais e futuros para segurança cibernética e proteção de dados, com grande enfoque na segurança do tratamento de dados pessoais e gestão de incidentes de segurança com violações de dados pessoais.

Este **Grupo de Cooperação**, terá como missão principal, apoiar e facilitar a cooperação estratégica entre os Estados-Membros no que se refere à segurança das redes e sistemas de informação, estabelecendo bases comuns de atuação para a gestão de riscos de cibersegurança, sem esquecer a garantia das liberdades das pessoas singulares, reforçando que todos os sistemas e serviços de cibersegurança, envolvidos na prevenção, deteção e resposta a ciberameaças deverão estar em conformidade com o atual quadro legal da União para a privacidade e proteção de dados.

O EDPS e a ENISA comprometem-se assim a apresentar um **plano estratégico para a capacitação e consciencialização das diferentes instituições da União Europeia,** sendo que esta abordagem conjunta e comum terá necessariamente por base de atuação, a missão de cada uma daquelas entidades – uma, a garantia dos direitos à privacidade e proteção de dados; a outra, a segurança das redes e sistemas da União, que permitirá a adoção de medidas tecnológicas capazes de melhorar a privacidade dos titulares e fortalecer as instituições da UE.

Na realidade, a cooperação entre estas entidades servirá, igualmente, para capacitar a resposta aos desafios futuros (e presentes!) em matéria de cibersegurança e privacidade, melhorando a segurança do tratamento de dados pessoais, a resposta que se pretende mais eficaz e assertiva na gestão de incidentes de violações de dados e ainda, – através de uma análise cuidada das tecnologias emergentes – aperfeiçoar e implementar de forma mais eficiente, os princípios da privacidade desde a conceção e por defeito.

Neste caminho, esta combinação de sinergias tornará ainda mais preponderante o **papel que a Cibersegurança e a Privacidade assumem** – e continuarão a assumir – seja no modelo de desenvolvimento económico que as Empresas e Organizações devem adotar, seja em prol da proteção dos seus ativos e dos titulares dos dados pessoais. Tem sido esta a nossa missão, alertar para o cumprimento e preparar as Empresas para saberem enfrentar os desafios da Era digital, investindo na tríade de segurança (pessoas, processos e tecnologia), consolidando uma abordagem holística, integrada e preventiva da Segurança da Informação.

Aguardemos assim, pela materialização efetiva do plano estratégico conjunto, com a certeza de que a segurança e a privacidade não mais serão atores principais de diferentes peças, mas antes, parceiros do mesmo palco democrático, o qual se pretende seguro.