Ciber resiliência europeia e o desafio da dependência digital estrangeira

dinheirovivo.pt/1807267774/ciber-resiliencia-europeia-e-o-desafio-da-dependencia-digital-estrangeira/

Muito se têm falado do termo “ciber resiliência”, não só no âmbito corporativo como também ao nível europeu, sendo este um tema bem presente na agenda da União Europeia (UE). Este conceito é definido pela NIST (National Institute of Standards and Technology) como “a capacidade de antecipar, resistir, recuperar e adaptar-se a condições adversas, tensões, ataques ou comprometimentos” nos vários domínios do ciberespaço. A verdade é que existe um fator que influencia esta capacidade de sermos mais ciber resilientes, ainda que passe algo despercebido a olhares menos atentos - a UE importa muitos produtos e serviços tecnológicos e de cibersegurança a operadores não pertencentes à União. No contexto atual, a dependência digital estrangeira representa um desafio significativo para a cibersegurança, e mais ainda para a soberania tecnológica da UE.

Embora a UE se esforce para estabelecer a sua soberania tecnológica e particularmente em termos de regulamentações, podemos aferir que a UE tem vindo a desenvolver um trabalho promissor e até mesmo pioneiro nesse sentido - exemplo disso é o Cyber Resilience Act e o AI Act – mas este ainda não é suficiente.

A ideia que fica é que os outros produzem e inovam, e nós (UE, leia-se) regulamentamos. E ainda bem que o fazemos, contudo, não podemos ser ingénuos e pensar que é suficiente ou que estamos menos dependentes da tecnologia de terceiros - nem tão pouco desviar o olhar dos notórios sinais de alerta em relação à segurança dos nossos dados.

Em particular, esta realidade prejudica a segurança da infraestrutura crítica da UE, que também é apoiada por complexas cadeias de abastecimento globais. O risco é ainda mais evidente quando operadores de fora da UE adquirem empresas europeias de cibersegurança. Esta dependência expõe a infraestrutura crítica da UE a vulnerabilidades significativas ao aumentar o risco de ciberataques, espionagem e sabotagem por parte de adversários estrangeiros. O desafio de proteger as infraestruturas críticas tem subjacente o desafio de a EU incrementar a sua própria autonomia e independência digital.

Outro fator a considerar está diretamente associado ao risco de ciberespionagem e vigilância por parte de governos estrangeiros. Esta preocupação é particularmente dramática se pensarmos em como pode minar a privacidade dos cidadãos europeus e até eventualmente, comprometer a segurança nacional.

A dependência de tecnologias estrangeiras limita também a própria autonomia tecnológica da UE, visto que, vai dificultar o desenvolvimento de capacidades próprias e a inovação em áreas críticas como, por exemplo, a inteligência artificial e a computação quântica. São já muitas as empresas europeias a implementar tecnologias como o Chatgpt (OpenAI) ou CoPilot (Microsoft); se fizermos o simples exercício de pensar a que empresas vamos buscar a tecnologia que utilizamos, quantas delas são europeias?

A UE dispõe de iniciativas e estratégias que têm como objetivo reforçar a autonomia tecnológica e aumentar a soberania digital em que, inclusive, se destaca a importância de desenvolver e adotar tecnologias da UE para reduzir a dependência estrangeira e reforçar a segurança e a privacidade dos dados. No entanto, alcançar a independência total neste domínio apresenta desafios significativos devido à natureza globalizada dos mercados tecnológicos e também porque muitos dos Estados-Membros da UE dependem de fornecedores estrangeiros de hardware, software e cloud. No fundo, estamos perante um paradoxo entre equilibrar a necessidade de tecnologia de vanguarda com a necessidade de proteger dados confidenciais.

A solução, apesar de não ser uma resposta óbvia, passará pelo investimento em capacidades domésticas ao estimular investimentos em pesquisa e desenvolvimento, quer da tecnologia quer ao nível de recursos humanos. Também a cooperação entre os vários Estados-membros é crucial, de modo a combater a fragmentação ao nível não só da inovação, mas também da aplicação de regulamentações. Regulamentações estas que, indubitavelmente, são também importantes para mitigar os riscos associados à dependência digital estrangeira e garantir a conformidade com padrões de cibersegurança e proteção de dados.

É efetivamente difícil encontrar um equilíbrio entre interesses económicos, inovação e segurança nacional. Ainda assim, é necessário ter presente que a ciber resiliência, vai muito mais além da regulamentação e envolve também uma certa ousadia coletiva em avançar, inovar e capacitar. Acima de tudo, é importante olhar os desafios como oportunidades - oportunidades para uma União Europeia mais segura, mais confiável e que quer estar na curva da onda da inovação.

Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense