

<input type="checkbox"/>	REQUERIMENTO	Número	/ (.ª)	Expeça - se
<input checked="" type="checkbox"/>	PERGUNTA	Número	/ XVII (1 .ª)	Publique - se
				O Secretário da Mesa

Assunto: Utilização de software de VPN da empresa israelita Check Point Software Technologies em universidades públicas portuguesas: implicações para a proteção de dados, soberania digital e responsabilidade ética das instituições

Destinatário: Ministro da Educação, Ciência e Inovação

Exmo. Senhor Presidente da Assembleia da República

Foi tornado público, em março de 2026, que a Universidade de Aveiro (UA) implementa o serviço de rede privada virtual (VPN) institucional com recurso ao software Capsule da empresa Check Point Software Technologies. A mesma solução é também utilizada pela Universidade do Porto, concretamente na Faculdade de Engenharia (FEUP) e na Faculdade de Ciências (FCUP), e pela Universidade Nova de Lisboa, na Faculdade de Ciências Sociais e Humanas (FCSH). As respetivas páginas de configuração técnica, de acesso público, confirmam sem ambiguidade a utilização deste software.

Uma VPN institucional é uma infraestrutura crítica de segurança: cria um túnel encriptado entre o dispositivo do utilizador (computador ou telemóvel) e a rede interna da universidade, sendo usada quotidianamente por docentes, investigadores, pessoal não docente e estudantes para acesso remoto a recursos, bases de dados científicas, sistemas de gestão académica e comunicações internas, incluindo email. A própria aplicação Capsule, quando instalada em dispositivos Android, exhibe ao utilizador o aviso: "a atividade da sua rede, incluindo dados de navegação e emails, está visível para o seu fornecedor de VPN."

Isso significa que, na arquitetura técnica adotada por estas universidades, potencialmente todo o tráfego de rede dos seus utilizadores passa por infraestrutura sob controlo da Check Point, sendo-lhe tecnicamente acessível.

A Check Point Software Technologies é uma das maiores empresas de cibersegurança do mundo, com sede em Telavive, Israel, e cotada no índice NASDAQ. A empresa foi fundada em 1993 por Gil Shwed, Marius Nacht e Shlomo Kramer. O fundador e durante 30 anos CEO, Gil Shwed, desenvolveu a tecnologia nuclear da empresa, a chamada stateful inspection, base do produto FireWall-1 e depois do VPN-1, enquanto servia na Unidade 8200 dos serviços de informação militares israelitas (Israel Defense Forces, IDF), conforme é reconhecido publicamente.

A Unidade 8200 é a maior unidade do exército israelita e o seu principal corpo de ciberinteligência e interceção de sinais (SIGINT), frequentemente comparada, em capacidades, à NSA dos EUA. É responsável por operações de espionagem eletrónica

massiva, interceção de comunicações e ciberguerra ofensiva. Entre os seus projetos mais conhecidos conta-se o malware Stuxnet, desenvolvido em cooperação com a NSA dos EUA para sabotar o programa nuclear iraniano.

A unidade é também reconhecida como a principal incubadora de empresas tecnológicas israelitas, com os seus quadros a fundar ou a liderar empresas como a Palo Alto Networks, a CyberArk, a NICE Systems e a NSO Group, esta última responsável pelo spyware Pegasus, utilizado para vigilância de jornalistas, ativistas e opositores políticos em todo o mundo.

Além das origens dos seus fundadores, a Check Point participa em consórcios com a Israel Aerospace Industries (IAI), uma das principais fabricantes de armamento e sistemas de armas não tripulados de Israel, e mantém relações institucionais com o aparelho de defesa e segurança israelita. Trata-se, por conseguinte, de uma empresa com elos orgânicos e estruturais ao complexo militar-industrial e de inteligência de Israel, elos que não se reduzem às trajetórias biográficas dos seus fundadores, mas que se inscrevem na própria arquitetura do setor tecnológico israelita, fortemente integrado com o Estado e as Forças Armadas.

Este quadro tem sido objeto de escrutínio parlamentar noutros países: em novembro de 2024, o Ministério da Defesa turco confirmou ao seu parlamento que as forças armadas turcas tinham abandonado os produtos Check Point desde junho de 2016, precisamente em resultado de preocupações de segurança associadas a estas ligações.

A utilização de um fornecedor de VPN com sede e infraestrutura fora da UE suscita questões jurídicas sérias no quadro do Regulamento Geral sobre a Proteção de Dados (RGPD - Regulamento UE 2016/679).

Por um lado, o artigo 35.º do RGPD impõe às entidades responsáveis pelo tratamento a obrigação de realizar uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) sempre que o tratamento em causa seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. O tratamento de dados de tráfego de rede, que pode incluir metadados de comunicação, conteúdos de e-mail e padrões de navegação, de milhares de membros da comunidade académica por um fornecedor externo não europeu preenche, manifestamente, esse critério.

Por outro lado, os artigos 44.º a 49.º do RGPD estabelecem um regime rigoroso para as transferências de dados pessoais para países terceiros. Israel beneficia de uma decisão de adequação da Comissão Europeia (adotada em 2011 e renovada), mas esta abrange unicamente o tratamento de dados por entidades sujeitas ao direito israelita de proteção de dados, e não o acesso por parte de serviços de informação ou forças armadas, que opera sob legislação própria e sem as garantias exigidas pelo direito europeu, conforme clarificado pelo Tribunal de Justiça da União Europeia no acórdão Schrems II (C-311/18, 2020) e na subsequente jurisprudência sobre adequação. A eventual transmissão de dados de comunicações académicas a entidades com ligações aos serviços de informação israelitas colocaria em causa a conformidade destas transferências com o RGPD.

Acresce que o software Capsule é proprietário e de código parcialmente fechado, o que impossibilita a auditoria independente do fluxo de dados e a verificação da efetiva aplicação das medidas técnicas de proteção declaradas.

Em contexto de conflito armado em curso em Gaza, com amplo reconhecimento internacional, incluindo pelo Tribunal Internacional de Justiça, de que as operações militares israelitas suscitam questões graves de conformidade com o direito internacional humanitário e com os direitos humanos, a contratação de serviços a empresas com ligações estruturais ao complexo militar-industrial israelita levanta questões éticas legítimas que as instituições de ensino superior não podem ignorar.

O Bloco de Esquerda não ignora que a rescisão unilateral de contratos em curso envolve limitações jurídicas. Mas considera que o Ministério da Educação e do Ensino Superior

tem a responsabilidade de garantir o cumprimento do RGPD e de promover, em sede de renovação ou renegociação contratual, a adoção de soluções tecnológicas soberanas, auditáveis e compatíveis com os valores das instituições públicas portuguesas e europeias.

Assim, ao abrigo das disposições constitucionais e regimentais aplicáveis, a Representação Parlamentar do Bloco de Esquerda ao Governo, através do Ministério da Educação, da Ciência e do Ensino Superior, as seguintes perguntas:

1. Tem o Ministério da Educação e do Ensino Superior conhecimento de que a Universidade de Aveiro, a Universidade do Porto (FEUP e FCUP) e a Universidade Nova de Lisboa (FCSH) utilizam o software Capsule da Check Point Software Technologies para os seus serviços de VPN institucionais? Existem outros estabelecimentos de ensino superior público que utilizem produtos da mesma empresa para serviços de rede ou segurança informática?

2. Foram realizadas, por parte das instituições em causa ou das tutelas competentes, Avaliações de Impacto sobre a Proteção de Dados (AIPD), nos termos do artigo 35.º do RGPD, relativamente à utilização deste software e ao tratamento de dados de tráfego de rede dos membros da comunidade académica? Em caso afirmativo, quais foram as conclusões e que medidas de mitigação foram adotadas?

3. Como avalia o Governo a conformidade das transferências de dados de tráfego de rede para infraestrutura da Check Point (empresa sediada em Israel e com ligações documentadas aos serviços de informação militares israelitas) com o regime de transferências internacionais de dados pessoais estabelecido nos artigos 44.º a 49.º do RGPD, nomeadamente à luz da jurisprudência do Tribunal de Justiça da UE fixada no acórdão Schrems II?

4. A Comissão Nacional de Proteção de Dados (CNPd) foi consultada ou pronunciou-se sobre a utilização deste tipo de software em instituições de ensino superior público? Tenciona o Governo promover essa consulta?

5. Considera o Governo que a utilização de software proprietário de código parcialmente fechado, desenvolvido por uma empresa com origem e ligações estruturais a uma unidade de ciberinteligência militar estrangeira, para infraestruturas críticas de rede em instituições de ensino superior público, é compatível com a Estratégia Nacional de Cibersegurança e com os objetivos de soberania digital da União Europeia, designadamente no quadro da Diretiva NIS 2 (Diretiva UE 2022/2555)?

6. Que orientações foram ou serão transmitidas pelo Ministério às instituições de ensino superior no sentido de garantir que, em sede de renovação ou nova contratação de serviços de VPN e segurança de rede, sejam adotadas soluções que assegurem: (a) o pleno controlo nacional ou europeu sobre os dados institucionais e dos utilizadores; (b) a possibilidade de auditoria independente do código e dos fluxos de dados; e (c) a conformidade com o RGPD e com a Diretiva NIS 2?

7. Perante as ligações documentadas da Check Point Software Technologies às forças armadas, aos serviços de informação e ao complexo industrial de defesa israelita, e no contexto do conflito armado em curso em Gaza, considera o Governo que as instituições de ensino superior devem ponderar critérios éticos e de responsabilidade em matéria de direitos humanos nos seus processos de contratação de serviços tecnológicos? Existem, ou estão previstas, orientações ministeriais nesse sentido?

Deputado(a)s
FABIAN FIGUEIREDO(BE)