SOUDNÍ DVŮR
EVROPSKÉ UNIE

TISKOVÁ ZPRÁVA č. 42/26
V Lucemburku dne 19. března 2026

Stanovisko generální advokátky ve věci C-354/24 | Elisa Eesti

Generální advokátka Ćapeta: Členské státy mohou odmítnout používání hardwaru a softwaru ve svých 2G-4G a 5G telekomunikačních infrastrukturách z důvodu, že výrobce těchto zařízení představuje riziko pro národní bezpečnost

Opatření přijatá na ochranu národní bezpečnosti členského státu však musí být podle unijního práva vždy přiměřená

V roce 2022 požádala společnost Elisa Eesti AS, estonský poskytovatel telekomunikačních služeb, estonské orgány o povolení používat hardware a software čínského výrobce telekomunikačních zařízení, Huawei, ve svých telekomunikačních sítích 2G-4G a 5G. Příslušné estonské orgány dospěly k závěru, že z důvodu „vysoce rizikové" povahy společnosti Huawei představuje tento hardware a software riziko pro národní bezpečnost Estonska. Toto rozhodnutí bylo napadeno u správního soudu v Tallinnu, který podal žádost o rozhodnutí o předběžných otázkách.

Ve svém stanovisku **generální advokátka Tamara Ćapeta navrhla, aby Soudní dvůr rozhodl, že členské státy v zásadě mohou vyloučit hardware a software ze své telekomunikační infrastruktury z důvodu, že výrobce těchto zařízení představuje riziko pro jejich národní bezpečnost**.

Generální advokátka však rovněž zdůraznila, že jakékoli rozhodnutí přijaté z důvodů národní bezpečnosti musí **podléhat soudnímu přezkumu**, a to i pokud jde o **jeho přiměřenost**. **Ačkoli se posouzení rizik může u výrobců zařízení ze třetích zemí lišit od posouzení rizik u unijních výrobců stejného zařízení, takové rozhodnutí nemůže být založeno na obecném podezření**. Naopak musí vycházet z konkrétního posouzení použití, k němuž je uvedené zařízení určeno, a s tím souvisejících rizik.

Za okolností projednávané věci generální advokátka rovněž zdůraznila, že relevantní pravidla unijního práva, evropský kodex pro elektronické komunikace[1], konkrétně stanoví určité požadavky na bezpečnost vnitrostátních telekomunikačních sítí a služeb. Na základě těchto požadavků unijního práva **se unijní a národní bezpečnostní zájmy sbližují.** V takové situaci mohou příslušné vnitrostátní orgány vycházet z posouzení rizik provedených unijními orgány, vnitrostátními a unijními institucemi[2].

Závěrem generální advokátka uvedla, že omezení používání hardwaru a softwaru z důvodu rizika, které tato zařízení představují pro bezpečnost Evropské unie a členských států, **nepředstavuje zbavení majetku, ale omezení užívání tohoto majetku ve smyslu čl. 17 odst. 1 Listiny**. V takovém případě má daná společnost v zásadě **nárok na náhradu škody pouze, pokud** vnitrostátní soud konstatuje, že **břemeno** vyplývající z tohoto druhu omezení **je nepřiměřené, byť nezbytné**.

rozhodovat. Rozsudek bude vydán později.

UPOZORNĚNÍ: Žádost o rozhodnutí o předběžné otázce umožňuje soudům členských států, aby v rámci sporu, který projednávají, položily Soudnímu dvoru otázky týkající se výkladu práva Unie nebo platnosti aktu Unie. Soudní dvůr nerozhoduje ve sporu před vnitrostátním soudem. Vnitrostátní soud musí věc rozhodnout v souladu s rozhodnutím Soudního dvora. Toto rozhodnutí je stejně závazné pro ostatní vnitrostátní soudy, které případně budou projednávat podobný problém.

Úplné znění stanoviska je zveřejněno na internetové stránce CURIA v den vyhlášení.

Kontaktní osoba pro tisk: Traian Moga ✆ (+352) 4303 3732.

Obrazové záznamy z přednesení stanoviska jsou dostupné na Europe by Satellite ✆ (+32) 2 2964106.

[1] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace.

[2] Viz zejména sdělení Komise o provádění souboru nástrojů pro kybernetickou bezpečnost sítí 5G, COM (2023) 4049 final.