Ministeriet for
Samfundssikkerhed og Beredskab

Dato: 23. september 2024
Kontor: Kontoret for Sikkerhed og Cyber
Sagsbeh: Akashdip Kaur Sahota
Sagsnr.: Sagsnummer
Dok.: Dokumentnummer

Notat til Folketingets Europaudvalg, Forsvarsudvalget og Udvalget for Digitalisering og IT om afgivelse af indlæg sag for EU-Domstolen, C-354/24, Elisa Eesti

1. Indledning

Forvaltningsdomstolen i Tallinn har forelagt EU-Domstolen (herefter Domstolen) seks præjudicielle spørgsmål om blandt andet fortolkningen af EU's direktiv 2018/1972[1], herunder direktivets artikel 1, stk. 3, litra c), sammenholdt med TEU[2] artikel 4, stk. 2, samt artikel 34 og artikel 36 i TEUF[3].

Domstolen skal blandt andet tage stilling til, hvorvidt en national ordning, som med henblik på beskyttelse af den nationale sikkerhed forpligter en udbyder af et offentligt tilgængeligt elektronisk kommunikationsnet og -tjeneste til at indhente en tilladelse til anvendelse af hardware og software i et offentligt tilgængeligt elektronisk kommunikationsnet og –tjeneste, er omfattet af anvendelsesområdet for direktiv 2018/1972. Såfremt dette er tilfældet, skal Domstolen tage stilling til, hvorvidt direktivets artikel 1, stk. 3, litra c), sammenholdt med TEU artikel 4, stk., 2, skal fortolkes således, at indførelsen af sådanne begrænsninger henhører under medlemsstatens enekompetence og udgør en ren national foranstaltning, hvilket vil betyde, at direktiv 2018/1972 ikke finder anvendelse.

[1]Europa-Parlamentets og Rådets direktiv 2018/1972 om oprettelse af en europæiske kodeks for elektronisk kommunikation.
[2]Traktaten om den Europæiske Union.
[3]Traktaten om Den Europæiske Unions Funktionsmåde.

Såfremt Domstolen vurderer, at sådanne begrænsninger henhører under medlemsstatens enekompetence og dermed udgør en ren national foranstaltning, skal Domstolen endvidere vurdere, om det er foreneligt med TEUF artikel 36 og proportionalitetsprincippet, hvis nationale tilladelsesordninger som dem i sagen omhandlede ikke forpligter forvaltningsmyndigheden til i forbindelse med risikovurderingen, at a) vurdere om de risici, der er knyttet til producenten, kan overføres på den konkrete hardware og software, b) at vurdere den konkrete hardwares og softwares funktionalitet, placering og betydning i forbindelse med udbydelsen af en kommunikationstjeneste, og c) at efterprøve, om de problemer, der er forbundet med producentens etableringsstat, kan overføres på producenten.

2. Sagens faktiske omstændigheder

Forelæggelsen for Domstolen udspringer af en konkret sag om tidsbegrænsning af anvendelsen af software og hardware fra Huawei for en kommunikationsudbyder. Tidsbegrænsningen blev meddelt af de relevante estiske myndigheder ud fra en betragtning om, at anvendelsen af udstyret udgør en risiko for den nationale sikkerhed.

Virksomheden Elisa Eesta AS (herefter sagsøger), indgav den 23. marts 2022 en ansøgning om tilladelse til brug af den 2G-4G-hardware og -software fra Huawei, som fandtes i selskabets offentligt tilgængelige elektroniske kommunikationsnet og –tjeneste, samt den 5G-hardware og -software fra Huawei, som fra den 1. juni 2022 skulle anvendes af sagsøgers offentligt tilgængelige elektronisk kommunikationsnet og –tjeneste.

Ved afgørelser af 27. oktober 2022 og 25. november 2022 fastslog det estiske cybersikkerhedsråd, at al den hardware og software, som var nævnt i sagsøgers ansøgning, udgjorde en risiko for den nationale sikkerhed, og meddelte sagsøger en brugstilladelse for 5G-funktionaliteten indtil den 31. december 2025 og for 2G-4G-funktionaliteten indtil den 31. december 2029. Sagsøger anlagde den 1. december 2022 et søgsmål ved forvaltningsdomstolen i Tallinn og gjorde i den forbindelse bl.a. gældende, at cybersikkerhedsrådets afgørelse af 27. oktober 2022 var ulovlig og udgjorde ekspropriation.

3. Relevante retsregler

Det følger af TEU artikel 4, stk. 2, at Den Europæiske Union skal respektere medlemsstaternes centrale statslige funktioner, herunder sikring af statens

territoriale integritet, opretholdelse af lov og orden samt beskyttelse af den nationale sikkerhed. National sikkerhed forbliver således den enkelte medlemsstats eneansvar.

Endvidere følger det af artikel 1, stk. 3, litra c), i direktiv 2018/1972, at direktivet ikke berører de tiltag, der gennemføres af medlemsstaterne ud fra hensynet til den offentlig orden og den offentlige sikkerhed og til forsvaret.

Det følger desuden af TEUF artikel 34, at kvantitative indførelsesrestriktioner såvel som alle foranstaltninger med tilsvarende virkning er forbudt mellem medlemsstaterne. TEUF artikel 34 er dog ikke til hinder for forbud eller restriktioner vedrørende indførsel, udførsel eller transit, som er begrundet i blandt andet hensynet til den offentlige sikkerhed jf. TEUF artikel 36. I sådanne tilfælde skal de nationale myndigheder dog godtgøre, at de pågældende bestemmelser overholder proportionalitetsprincippet, og således være tilstrækkeligt begrundet og forholdsmæssige.[4]

4. Regeringens interesse i sagen

Regeringens interesse i sagen skal ses i lyset af, at Domstolens besvarelse af spørgsmålene kan få betydning for dansk lovgivning, navnlig lov om leverandørsikkerhed i den kritiske teleinfrastruktur (herefter telesikkerhedsloven)[5].

I Danmark eksisterer en lignende ordning som den estiske. Center for Cybersikkerhed (herefter CFCS) kan således med hjemmel i telesikkerhedsloven i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis opretholdelse af aftalen vurderes at udgøre en trussel mod statens sikkerhed. CFCS kan endvidere, med hjemmel i telesikkerhedsloven, i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, samt forbyde at anvende sådanne netkomponenter, systemer og værktøjer, der er leveret, hvis opretholdelse

[4] *Franzén,* C-189/95, EU:C1997:504, dom af 23, oktober 1997, præmis 75 og *Rosengren m.fl.,* C-170/04, EU:C:2007:313, dom af 5. juni 2007, præmis 50.
[5] Lov nr 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur.

af aftalen eller anvendelsen af de pågældende netkomponenter, systemer og værktøjer vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Forbud efter telesikkerhedsloven forudsætter, at CFCS konkret har vurderet, at hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger end et forbud.

Hvis Domstolen vurderer, at en ordning, som den i sagen omhandlede, henhører under medlemsstatens enekompetence og udgør en ren national foranstaltning, jf. TEU artikel 4, stk. 2, hvorpå bestemmelserne i direktiv 2018/1972 ikke finder anvendelse, skal Domstolen vurdere, om den estiske tilladelsesordning er forenelig med TEUF artikel 36 og proportionalitetsprincippet.

Domstolens vurdering heraf kan få betydning for, hvilke kriterier medlemsstaternes myndigheder (i Danmark, CFCS) skal lægge vægt på i forbindelse med sådanne vurderinger af hensyn til den nationale sikkerhed, herunder kriterier vedrørende risikovurderinger og deres nærmere konkretiseringsgrad. Det bemærkes, at sådanne vurderinger efter omstændighederne kan basere sig på klassificerede oplysninger.

Den præjudicielle forelæggelse kan således få betydning for CFCS' muligheder for at varetage hensynet til statens sikkerhed efter reglerne i telesikkerhedsloven. Besvarelsen vil derudover generelt få betydning for forståelsen af EU-rettens anvendelsesområde i relation til medlemsstaternes eneansvar for national sikkerhed, jf. TEU artikel 4, stk. 2.

På baggrund af ovenstående vil regeringen i sagen argumentere for, at national sikkerhed efter TEU artikel 4, stk. 2, er den enkelte medlemsstats eneansvar, hvorfor direktiv 2018/1972 ikke finder anvendelse for nationale ordninger, der har til formål at sikre den nationale sikkerhed, herunder i relation til telesikkerhed. Sidstnævnte udgør et vigtigt redskab til at kunne sikre den kritiske teleinfrastruktur mod trusler fra andre lande.

Regeringen vil derudover argumentere for, at sådanne nationale ordninger skal overholde EU-rettens regulering om fri bevægelighed og de generelle EU-retlige principper, herunder proportionalitetsprincippet. Regeringen vil i forlængelse heraf argumentere for, at TEUF artikel 34 og 35 ikke er til hinder for begrænsninger, der er begrundet i hensynet til den nationale sikkerhed, jf. TEUF artikel 36, så længe de nationale forskrifter er nødvendige for at virkeliggøre det tilsigtede formål, og dette mål ikke kan

nås ved hjælp af forbud eller begrænsninger, der er mindre vidtrækkende. Regeringen vil i den forbindelse argumentere for, at det tilkommer medlemsstaterne at træffe de nødvendige foranstaltninger til at opretholde deres indre og ydre sikkerhed.

Afslutningsvist skal det bemærkes, at der verserer en sag ved Østre Landsret, hvor TDC NET har indbragt en afgørelse om forbud meddelt af CFCS efter telesikkerhedsloven for retten, herunder med påstand om erstatning for ekspropriation.