Datum van inontvangstneming	:	15/07/2024

Zaak C-354/24

Samenvatting van het verzoek om een prejudiciële beslissing overeenkomstig artikel 98, lid 1, van het Reglement voor de procesvoering van het Hof van Justitie

Datum van indiening:

15 mei 2024

Verwijzende rechter:

Tallinna Halduskohus (Estland)

Datum van de verwijzingsbeslissing:

15 mei 2024

Verzoekende partij:

Elisa Eesti AS

Verwerende partijen:

Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu

Tarbijakaitse ja Tehnilise Järelevalve Amet

Voorwerp van het hoofdgeding

Beroep waarbij Elisa Eesti AS verzoekt om het besluit van de Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu (raad voor cyberbeveiliging van het veiligheidscomité van de regering van de Republiek) van 27 oktober 2022 in zijn geheel en het besluit van de Tarbijakaitse ja Tehnilise Järelevalve Amet (autoriteit voor consumentenbescherming en technische controle) van 25 november 2022 gedeeltelijk nietig te verklaren en verweerders dienovereenkomstig te verplichten.

Voorwerp en rechtsgrondslag van de verwijzingsbeslissing

Het verzoek om een prejudiciële beslissing krachtens artikel 267, tweede alinea, VWEU betreft de uitlegging van richtlijn 2018/1972 van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie, met name artikel 1, lid 3, onder c), gelezen in samenhang met

artikel 4, lid 2, VEU, alsmede artikel 12, lid 1, van deze richtlijn, artikelen 34 en 36 VWEU alsmede artikel 17, lid 1, tweede zin, van het Handvest van de grondrechten van de Europese Unie.

Prejudiciële vragen

1) Valt een geheel van nationale wettelijke regelingen (§ 87[3], leden 2, 3, 6, 7 en 8, § 87[4], leden 1 tot en met 4, en § 196[5], leden 1 tot en met 4, van de Elektroonilise side seadus [wet inzake elektronische communicatie; hierna: „ESS”], op grond waarvan een communicatieonderneming ter waarborging van de nationale veiligheid een machtiging moet verkrijgen voor het gebruik van hardware en software in haar communicatienetwerk, binnen het toepassingsgebied van richtlijn 2018/1972 van het Europees Parlement en de Raad van 20 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie?

2) Indien bovenstaande vraag bevestigend wordt beantwoord: moet artikel 1, lid 3, onder c), [van richtlijn 2018/1972], gelezen in samenhang met artikel 4, lid 2, [VEU,] aldus worden uitgelegd dat de invoering van dergelijke beperkingen tot de uitsluitende bevoegdheid van de lidstaat behoort en een zuiver nationale maatregel vormt waarop de bepalingen van richtlijn 2018/1972 niet van toepassing zijn?

3) Indien de [tweede] vraag ontkennend wordt beantwoord: vormt een geheel van nationale wettelijke regelingen (§ 87[3], leden 2, 3, 6, 7 en 8, § 87[4], leden 1 tot en met 4, en § 196[5], leden 1 tot en met 4, ESS), op grond waarvan het een communicatieonderneming niet is toegestaan hardware en software in haar communicatienetwerk te gebruiken zonder daarvoor van een administratieve autoriteit een machtiging voor het gebruik van deze hardware en software te verkrijgen, een beperking van de vrijheid om elektronischecommunicatienetwerken en -diensten aan te bieden in de zin van artikel 12, lid 1, [van richtlijn 2018/1972]?

4) Indien de [derde] vraag bevestigend wordt beantwoord: moeten dergelijke nationale wettelijke regelingen buiten toepassing worden gelaten wanneer zij niet vooraf overeenkomstig artikel 12, lid 1, van [richtlijn 2018/1972] ter kennis zijn gebracht van de Europese Commissie?

5) Indien de [tweede] vraag bevestigend wordt beantwoord: is het verenigbaar met artikel 36 VWEU en het evenredigheidsbeginsel dat een nationale wettelijke regeling ter waarborging van de nationale veiligheid een communicatieonderneming verplicht een machtiging te verkrijgen voor het gebruik van hardware en software in haar communicatienetwerk, en dat deze regeling de administratieve autoriteit niet verplicht om bij de beoordeling van het gevaar dat uitgaat van hardware en software met een hoog risico, a) na te gaan of de aan de fabrikant verbonden risico’s ook gelden voor de specifieke hardware en software, b) de functionaliteit, de locatie en het

belang van de specifieke hardware en software te beoordelen in het kader van het aanbieden van een communicatiedienst, en c) te onderzoeken of problemen die verband houden met de staat van vestiging van de fabrikant, ook gelden voor de fabrikant?

6) Is er sprake van ontneming van eigendom in de zin van artikel 17, lid 1, tweede zin, van het Handvest van de grondrechten van de Europese Unie indien het gebruik van hardware of software die reeds in het communicatienetwerk aanwezig was en actief in het communicatienetwerk werd gebruikt, wordt toegestaan voor een kortere periode dan de gebruiksduur van die hardware of software en de betrokken hardware of software rechtmatig is verworven?

Aangevoerde Unierechtelijke bepalingen

Verdrag betreffende de Europese Unie, artikel 4, lid 2

Verdrag betreffende de werking van de Europese Unie, artikel 36

Handvest van de grondrechten van de Europese Unie (hierna: „Handvest"), artikel 17, lid 1, tweede zin

Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie, artikel 1, lid 3, onder c), en artikel 12, lid 1

Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, artikel 5, lid 1

Aangevoerde nationale bepalingen

Elektroonilise side seadus (wet inzake elektronische communicatie; hierna: „ESS"), § 87^3, leden 2, 3, 6, 7 en 8, § 87^4, leden 1 tot en met 4, en § 196^5, leden 1 tot en met 4

Volgens § 87^3, lid 2, ESS kan de in een communicatienetwerk gebruikte hardware of software de nationale veiligheid in gevaar brengen wegens het hoge risico dat de fabrikant of de aanbieder van onderhouds- of ondersteuningsdiensten vormt (punt 1), of wegens het risico dat de technische kenmerken of de configuratie van de hardware of software vormen (punt 2).

In § 87^3, lid 3, punten 1 tot en met 12, ESS worden de omstandigheden opgesomd die verband houden met de staat waar de fabrikant of aanbieder van onderhouds- of ondersteuningsdiensten gevestigd is en die bij de beoordeling van

de hardware of software met het oog op de nationale veiligheid als een hoog risico worden aangemerkt.

Volgens § 87^3, lid 6, ESS is een communicatieonderneming verplicht om voor het gebruik van de hardware of software van een communicatienetwerk een machtiging te verkrijgen van de Tarbijakaitse ja Tehnilise Järelevalve Amet (autoriteit voor consumentenbescherming en technische controle; hierna: „TTJA"). § 87^3, lid 7, bepaalt dat de regering van de Republiek de omvang van de verplichting om een gebruiksmachtiging te verkrijgen, de nadere voorschriften, de termijn en de modaliteiten van de procedure alsmede de bijzonderheden van de duur van de gebruiksmachtiging bij verordening regelt. Krachtens lid 8 houdt de regering van de Republiek bij de vaststelling van de verordeningen rekening met het belang van het communicatienetwerk, zijn hardware of software en de communicatiedienst die via dit netwerk wordt geleverd, alsmede met de mogelijke gevaren die deze voor de nationale veiligheid meebrengen.

§ 87^4 ESS beschrijft de procedure voor het verlenen van de machtiging voor het gebruik van de hardware of software.

§ 196^5 ESS regelt de wijze van toepassing van de §§ 87^3 en 87^4 van deze wet.

Vabariigi Valitsuse 22.06.2006 määrus nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded" (verordening nr. 140 van de regering van de Republiek van 22 juni 2006 „voorschriften voor het aanbieden van communicatiediensten en technische eisen voor communicatienetwerken")

Korte uiteenzetting van de feiten en de procedure

1 Elisa Eesti AS (hierna: „Elisa Eesti"), waarvan de moedermaatschappij de Finse vennootschap Elisa Oyj is, is een van de drie eigenaren van het in Estland opgezette nationale mobieletelefonienetwerk. Deze drie communicatieondernemingen zijn aanbieders van kritieke diensten en voor de hardware en software die binnen hun mobiele netwerken wordt gebruikt, is sinds 1 februari 2022 een machtiging vereist overeenkomstig verordening nr. 140 van de regering van de Republiek van 22 juni 2006.

2 Het mobiele netwerk van Elisa, dat bestaat uit meer dan duizenden basisstations, is gebaseerd op de hardware en software van Huawei. De mobiele generaties (2G, 3G, 4G, 5G) zijn technisch met elkaar verbonden.

3 Op 23 maart 2022 heeft Elisa bij de TTJA een aanvraag ingediend voor een machtiging voor het gebruik van de bestaande 2G- tot 4G-hardware en -software van Huawei in haar communicatienetwerk, alsook van 5G-hardware en -software van Huawei die vanaf 1 juni 2022 in het communicatienetwerk van Elisa zou worden ingezet.

4 Bij besluit van 27 oktober 2022 oordeelde de Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu (raad voor cyberbeveiliging van het veiligheidscomité van de regering van de Republiek; hierna: KJN) op basis van § 87^4, lid 2, ESS dat alle hardware en software waarnaar in de aanvraag van Elisa wordt verwezen, een bedreiging vormt voor de nationale veiligheid, en stelde de TTJA voor om een gebruiksmachtiging voor de 5G-functionaliteit tot en met 31 december 2025 en voor de 2G- tot 4G-functionaliteit tot en met 31 december 2029 te verlenen.

5 De TTJA heeft het besluit op 25 november 2022 aan Elisa toegezonden en voornoemde gebruiksmachtigingen verleend voor de door de KJN gespecificeerde perioden. Onder verwijzing naar de motivering van het besluit van de KJN heeft de TTJ vastgesteld dat alle in de machtigingsaanvraag van Elisa vermelde hardware en software de nationale veiligheid in gevaar bracht.

6 Elisa heeft op 1 december 2022 beroep ingesteld bij de Tallinna Halduskohus (bestuursrechter in eerste aanleg Tallinn, Estland), strekkende tot volledige nietigverklaring van het besluit van de KJN van 27 oktober 2022 en gedeeltelijke nietigverklaring van het besluit van de TTJA van 25 november 2022, en tot overeenkomstige verplichting van verweerders.

Voornaamste argumenten van partijen in het hoofdgeding

7 Elisa stelt dat de bestreden besluiten onrechtmatig zijn, beoordelingsfouten bevatten, in strijd zijn met het toepasselijke recht en haar grondrechten onevenredig schenden. Wanneer een onderneming met terugwerkende kracht in het belang van de nationale veiligheid, dat wil zeggen in het algemeen belang, wordt verboden bepaalde hardware en software te gebruiken, komt dit in wezen neer op een onteigening die onmiddellijk en op passende wijze moet worden gecompenseerd. De KJN en de TTJA hebben ten onrechte geoordeeld dat de beperking van de geldigheidsduur van de gebruiksmachtiging geen significante gevolgen heeft voor de communicatiemarkt en de mededinging.

8 De KJN en de TTJA hebben § 87^3, leden 2 en 3, ESS onjuist uitgelegd. Zij hebben de waarschijnlijkheid van het vermeende gevaar en de nabijheid van het ontstaan van daarmee verband houdende schade en de omvang daarvan niet onderzocht. Bovendien was het besluit van de KJN niet gebaseerd op het begrip „gevaar”, maar op een „vermoeden van gevaar”.

9 Verweerders hebben volgens Elisa niet aangetoond dat er sprake is van een gevaar voor de nationale veiligheid (§ 87^4, lid 4, ESS). Uit de mededeling van de Europese Commissie van 15 juni 2023 blijkt dat slechts tien van de 27 lidstaten beperkingen hebben toegepast op aanbieders met een hoog risico of hen hebben uitgesloten van hun 5G-netwerken.

10 In het besluit van de KJN is bij de vaststelling van de risicodrempel geen rekening gehouden met de ernst van de eventuele schending van de grondrechten van Elisa.

De enige mogelijke manier om de 5G-generatie aan te bieden, is vandaag de dag deze met behulp van bestaande interfaces op het bestaande 2G/3G/4G-netwerk op te bouwen als een 5G NSA-oplossing. Hierbij is het noodzakelijk dat de 5G-hardware en -software en de 4G-hardware en -software van dezelfde fabrikant afkomstig zijn.

11 De uitrol van mobiele netwerken wordt jaren van tevoren gepland. Voor Elisa was een van de belangrijkste voorwaarden voor de selectie van een aanbieder in 2014 dat de volgende generatie netwerken, 5G, kon worden opgebouwd op de 4G-hardware en -software die bij de geselecteerde aanbieder (Huawei) was besteld.

12 Om 5G-hardware en -software van een alternatieve aanbieder te installeren, zou Elisa de bestaande 4G-hardware en -software van Huawei moeten vervangen. De kosten voor het vervangen van de volledige 4G-hardware en -software vormen schade voor Elisa.

13 De bestreden administratieve handelingen zijn maatregelen van gelijke werking als kwantitatieve invoerbeperkingen die in strijd zijn met artikel 34 VWEU. De bestreden administratieve handelingen voldoen niet aan de bewijsstandaard die volgens de rechtspraak van het Hof van Justitie vereist is om het vrije verkeer van goederen te beperken: het bestaan van een feitelijk, rechtstreeks en voldoende ernstig risico dat concreet en in elk afzonderlijk geval wordt aangetoond.[1] De KJN en de TTJA hebben niet aangetoond dat het verbod op het gebruik van hardware en software van Huawei in het communicatienetwerk van Elisa een passende, noodzakelijke en evenredige maatregel is om het gestelde gevaar te voorkomen. De bestreden administratieve handelingen beletten Elisa om uit Finland afkomstige hardware en software van Huawei te blijven betrekken, aangezien de hardware en software van Huawei op grond van die handelingen in Estland niet voor het beoogde doel kunnen worden gebruikt.

14 In de bestreden administratieve handelingen wordt volgens Elisa niet uitgelegd welke van de in artikel 36 VWEU genoemde doelstellingen volgens verweerders een beperking van het vrije verkeer van goederen rechtvaardigen en waarom de beperking een evenredige maatregel vormt om het nagestreefde doel te bereiken.[2]

15 De Estse Staat was verplicht om overeenkomstig artikel 5, lid 1, van richtlijn 2015/1535 de ontwerpen tot wijziging van de ESS en van het op 1 februari 2022 krachtens verordening nr. 140 in werking getreden stelsel van

[1] Zie arresten van het Hof van Justitie van de Europese Unie van 18 november 1979, Denkavit Futtermittel, 251/78, EU:C:1979:252 punt 24, 8 mei 2003, ATRAL, C-14/02, EU:C:2003:265 punten 66-69, en 23 december 2015, Scotch Whisky Association e.a., C-333/14, EU:C:2015:845, punt 53.

[2] Arrest van het Hof van Justitie van 10 juli 1984, Campus Oil e.a., 72/83, EU:C:1984:256.

gebruiksmachtigingen voor te leggen aan de Europese Commissie.[3] Estland heeft de Commissie niet in kennis gesteld van het op 27 september 2021 ingediende wetsontwerp waarbij de §§ 87^3 tot en met 87^5 en § 196^5 met het oog op de regeling van de gebruiksmachtigingen werden ingevoegd in de ESS. De rechtsgrondslag voor de wijzigingen van de bepalingen van verordening nr. 140 betreffende de gebruiksmachtiging waren § 87^3, leden 5 en 6, en § 87^5, lid 5, ESS. Wegens schending van de kennisgevingsplicht moeten de wettelijke regelingen inzake de gebruiksmachtiging van zowel de ESS als verordening nr. 140 buiten toepassing worden gelaten, aangezien zij zonder rechtsgrondslag zijn vastgesteld.

16 Volgens Elisa zijn de bestreden administratieve handelingen in strijd met artikel 12, lid 1, van richtlijn 2018/1972. De beperkingen waren niet noodzakelijk voor de bescherming van de openbare orde of de openbare veiligheid en waren onvoldoende gemotiveerd.[4]

17 De bestreden administratieve handelingen zijn in strijd met de algemene beginselen van het Unierecht: het beginsel van bescherming van het gewettigd vertrouwen, het beginsel van gelijke behandeling, het fundamentele recht op eigendom, de vrijheid van ondernemerschap en het recht op behoorlijk bestuur, dat het recht om te worden gehoord, het recht op een onpartijdig en eerlijk proces en het beginsel van onderzoek in administratieve procedures omvat. In zijn besluit heeft de TTJA zich voor 100 % gebaseerd op de voorstellen en de redenering van de KJN als politiek orgaan, aldus Elisa.

18 De administratieve handeling van de TTJA heeft tot gevolg dat Huawei's 4G-hardware en -software de facto wordt onteigend door die technologie onbruikbaar te maken (schending van het Handvest), dat Elisa ongelijk wordt behandeld ten opzichte van communicatieondernemingen die geen hardware en software van Huawei in hun netwerk hebben (schending van artikel 20 van het Handvest), en dat het gewettigd vertrouwen van Elisa ernstig wordt geschonden.

19 Volgens Elisa handelen verweerders overduidelijk in strijd met het verbod om op tegenstrijdige wijze te handelen. De administratieve handelingen zijn formeel onwettig.

20 Verweerders verzetten zich tegen het beroep en concluderen tot verwerping ervan.

21 De besluiten zijn ten gronde wettig. Verweerders hebben § 87^3, leden 2 en 3, ESS correct toegepast. De beoordeling door de KJN van het gevaar voor de nationale veiligheid dat de staat van de fabrikant vertegenwoordigt, vormt een risicobeoordeling en geen feitelijke vaststelling. In casu is het gevaar voor de

[3] Zie arrest van het Hof van Justitie van 30 april 1996, CIA Security International, C-194/94, EU:C:1996:172, punt 55.

[4] Indien een nationale wettelijke bepaling in strijd is met het Unierecht, is ook een overheidsinstantie verplicht deze buiten toepassing te laten (zie arrest van 22 juni 1989, Costanzo, 103/88, EU:C:1989:256, punt 31).

nationale veiligheid overeenkomstig § 87[3], lid 2, punt 1, ESS vastgesteld wegens het hoge risico dat de fabrikant vertegenwoordigt, en niet overeenkomstig § 87[3], lid 2, punt 2, ESS, dat wil zeggen op grond van het risico dat de technologie zelf vertegenwoordigt.

22 In het kader van het Unierecht valt de nationale veiligheid onder de uitsluitende bevoegdheid van elke lidstaat. Bovendien maakt het concept van nationale veiligheid geen onderscheid tussen verschillende gevarenniveaus; het gevaar moet veeleer op zijn minst voorzienbaar of te verwachten zijn.

23 Verweerders hebben hun beoordelingsbevoegdheid niet geschonden en hebben rekening gehouden met alle relevante omstandigheden. De KJN heeft een risico vastgesteld met betrekking tot alle twaalf criteria die zijn opgesomd in § 87[3], lid 3, ESS, heeft andere relevante omstandigheden in aanmerking genomen en is na een algemene beoordeling tot de conclusie gekomen dat Elisa een machtiging aanvroeg voor het gebruik van hardware en software die de nationale veiligheid in gevaar bracht. Daarom kon er geen gebruiksmachtiging worden verleend na 31 december 2029 voor 2G tot 4G en na 31 december 2025 voor 5G (§ 196[5] ESS). Dit is de maximale overgangsperiode waarin de wet voorziet, en verweerders beschikken niet over enige discretionaire bevoegdheid om de aanvraag voor een langere periode in te willigen. Bij de toekenning van de overgangsperiode is rekening gehouden met de aan Elisa toe te rekenen omstandigheden.

24 De rechterlijke toetsing van het beoordelingsbesluit is beperkt tot de zogenoemde toetsing van de redelijkheid en doeltreffendheid, waarbij met name wordt nagegaan of de administratieve autoriteit rekening heeft gehouden met de doelstellingen van de wet, de algemene rechtsbeginselen en de relevante feiten en of de beoordeling is verricht met inachtneming van de beoordelingscriteria en -beperkingen (§ 87[3], leden 2 en 3, § 87[4], leden 2 tot en met 4, en § 196[5], leden 2 en 4, ESS). Hoewel de uitlegging van het onbepaalde rechtsbegrip nationale veiligheid aan rechterlijke toetsing is onderworpen, moet er rekening mee worden gehouden dat het ook gaat om een gebied waarvoor specifieke kennis over de nationale veiligheid en technische deskundigheid nodig zijn, en dat het recht en de verplichting om in de regelingen vervatte onbepaalde rechtsbegrippen uit te leggen, toekomen aan het bestuursorgaan dat verantwoordelijk is voor de procedure.

25 Volgens verweerders zijn de besluiten formeel wettig. De TTJA heeft de motiveringsplicht niet geschonden. De bevoegdheid om te beslissen of hardware of software de nationale veiligheid in gevaar brengt, komt uitsluitend toe aan de KJN. In dit verband moet het overleg met de KJN worden beschouwd als een voorbereidende administratieve handeling, aangezien de KJN een omstandigheid vaststelt die relevant is voor de eindbeslissing in de zaak – te weten of het gaat om hardware of software met een hoog risico die de nationale veiligheid in gevaar brengt. De beoordeling door de KJN is gebaseerd op het veiligheidsrisico waarvan hij kennis heeft gekregen en dat niet opnieuw mag worden beoordeeld door de

TTJA. Wanneer de KJN een voorstel inzake de voorwaarden heeft gedaan, is dit voorstel bindend voor de TTJA bij het verlenen van de gebruiksmachtiging.

26 De nationale wettelijke regeling is in overeenstemming met het Unierecht. De maatregelen worden gerechtvaardigd door de noodzaak om de nationale veiligheid te beschermen. Uit de door Elisa aangehaalde rechtspraak blijkt niet dat de werking van de kritieke diensten zonder uitzondering onder de openbare veiligheid in de zin van artikel 36 VWEU valt. De vaststelling van de wezenlijke belangen van de nationale veiligheid valt onder de uitsluitende bevoegdheid van de staat. In een vonnis heeft een Zweedse bestuursrechter geoordeeld dat een nationale regeling op grond waarvan het gebruik van Huawei-apparatuur in een communicatienetwerk kan worden verboden, noodzakelijk was om de nationale veiligheid van Zweden te waarborgen. Overeenkomstig aanbeveling (EU) 2019/534 van de Europese Commissie hebben de lidstaten het recht om aanbieders of leveranciers van hun markten te weren om redenen van nationale veiligheid. De KJN heeft terecht vastgesteld dat er een gevaar voor de nationale veiligheid bestaat.

27 De in de ESS vastgestelde bewijsstandaard is in overeenstemming met het Unierecht, ook al dienen de maatregelen (wettelijke regelingen) het door Elisa aangevoerde belang van de openbare veiligheid. Uit de rechtspraak van het Hof van Justitie van de Europese Unie volgt niet de door Elisa gestelde bewijslast; veeleer moet worden onderzocht of het gevaar voor de nationale veiligheid reëel (waarschijnlijkheid) en voldoende ernstig (ernst van de schade) is.[5]

28 Aan de informatieplicht is voldaan. Estland heeft de Europese Commissie in kennis gesteld van het stelsel van gebruiksmachtigingen[6] en hoefde de latere wijzigingen niet bij de Commissie te melden, hetzij omdat deze wijzigingen niet significant waren, hetzij omdat deze wijzigingen slechts in een versoepeling ten opzichte van het oorspronkelijke ontwerp voorzagen. De in artikel 5, lid 1, derde alinea, van richtlijn 2015/1535 neergelegde verplichting moet worden beoordeeld in het licht van het doel van deze richtlijn, namelijk de bescherming van het vrije verkeer van goederen door een preventieve controle, hetgeen wordt gewaarborgd door de procedure van onderzoek van het ontwerp voor een technisch voorschrift door de Commissie en de lidstaten.[7] Een lidstaat is niet verplicht een ontwerp voor een administratieve handeling mee te delen.[8]

5 Arrest van de administratieve kamer van de Riigikohus (hoogste rechterlijke instantie) van 19 februari 2019 nr. 3-17-1545, punt 19. Elektronisch beschikbaar: https://www.riigikohus.ee/et/lahendid?asjaNr=3-17-1545/81.

6 https://technical-regulation-information-system.ec.europa.eu/et/notification/15441.

7 Zie arresten van het Hof van Justitie van 10 juli 2014, [redacted] e.a., C-307/13, EU:C:2014:2058, punten 41-43, en 15 april 2010, [redacted] C-433/05, EU:C:2010:184, punten 46-49.

8 Zie arrest [redacted] e.a., C-307/13, punt 44-46.

29 Verweerders zijn het niet eens met het standpunt van Elisa over de schending van de informatieplicht door Estland. De informatierichtlijn is niet van toepassing op de litigieuze bepalingen (richtlijn 2015/1535, artikel 1, lid 3). De bepalingen van de ESS, die eisen stellen aan communicatienetwerken en -diensten om de nationale veiligheid te waarborgen en de bevoegde nationale regelgevende instanties de bevoegdheid verlenen om tijdens de machtigingsprocedure bindende richtsnoeren vast te stellen (§§ 87^3 tot en met 87^5 en 196^5 ESS), vallen binnen het toepassingsgebied van richtlijn 2002/21/EG (artikel 13 bis, leden 1 en 2, van richtlijn 2002/21/EG [herschikt bij richtlijn 2018/1972][9] [artikel 40, lid 1, van richtlijn 2018/1972] en artikel 13 ter, leden 1 en 2, van richtlijn 2002/21/EG [artikel 41 van richtlijn 2018/1972]). Zelfs als de informatierichtlijn van toepassing zou zijn, zouden de uitzonderingen op de informatieplicht waarin de richtlijn voorziet, gelden.[10]

30 Artikel 12, lid 1, van richtlijn 2018/1972 is niet relevant, voor zover het de algemene machtiging voor elektronischecommunicatienetwerken en -diensten regelt die is gebaseerd op de ingetrokken richtlijn 2002/20/EG en niet op richtlijn 2002/21/EG. Artikel 12, lid 1, van richtlijn 2018/1972 is omgezet in de §§ 3 en 4 ESS. Volgens verweerders was ook Elisa van mening dat de invoering van het stelsel van gebruiksmachtigingen ter waarborging van de nationale veiligheid geen verband hield met de omzetting van richtlijn 2018/1972.

31 De bestreden administratieve handeling is niet in strijd met de algemene beginselen van de Unie. Uit de arresten van het Hof van Justitie[11] blijkt niet de door Elisa gestelde afwijking ten opzichte van het nationale recht of de nationale rechtspraak in het licht van het evenredigheidsbeginsel. De nationale veiligheid is ook volgens de rechtspraak van het Hof van Justitie[12] een legitiem en zeer belangrijk doel van de beperking van de grondrechten. Het ontbreken van een compensatieregeling maakt de administratieve handeling niet onwettig. Het gaat niet om een onteigening. Het vereiste van een gebruiksmachtiging is evenredig aan het legitieme doel. Het is niet in strijd met het grondrecht van de communicatieonderneming op gelijke behandeling in de zin van artikel 20 van het Handvest, aangezien het op dezelfde wijze van toepassing is op eenieder.

9 Richtlijn 2002/21/EG werd omgezet in Ests recht door de ESS in de versie die van toepassing is vanaf 1 januari 2005, en richtlijn 2018/1972 door de ESS in de versie die van toepassing is vanaf 1 februari 2022.

10 Zie aanbeveling (EU) 2019/534 van de Commissie, artikel 26; richtlijn 2015/1535, artikel 7.

11 Arresten van het Hof van Justitie van 6 oktober 2020 2020, Commissie/Hongarije (hogeronderwijsopleiding), C-66/18, EU:C:2020:792, punt 179, 18 juni 2020, Commissie/Hongarije (transparantie van verenigingen), C-78/18, EU:C:2020:476, punt 77, en 10 februari 2009, Commissie/Italië, C-110/05, EU:C:2009:66, punt 62.

12 Zie arrest van 5 april 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, punten 57-58.

32 Verweerster heeft het beginsel van behoorlijk bestuur niet geschonden. De communicatieonderneming kan geen gewettigd vertrouwen hebben in de handhaving van de status quo.[13]

Korte uiteenzetting van de motivering van de verwijzing

33 Partijen zijn het oneens over de vraag of de bestreden administratieve handelingen verenigbaar zijn met onder meer het Unierecht, te weten artikel 5, lid 1, van richtlijn 2015/1535, artikel 12, lid 1, van richtlijn 2018/1972, de artikelen 34 en 36 VWEU alsmede artikel 17, lid 1, tweede zin, van het Handvest.

34 Het onderhavige geschil betreft geen zuiver nationale maatregel,[14] aangezien de moedermaatschappij van Elisa Oyj is, die in een andere lidstaat is gevestigd.

Richtlijn 2015/1535

35 Partijen zijn het oneens over de vraag of de bestreden nationale bepalingen moeten worden aangemerkt als technische voorschriften in de zin van artikel 1, lid 1, onder f), van richtlijn 2015/1535 en of zij vooraf aan de Commissie moesten worden medegedeeld. Volgens de rechtspraak van het Hof van Justitie[15] kan het gaan om bepalingen van de vierde categorie van artikel 1, lid 1, onder f) („wettelijke en bestuursrechtelijke bepalingen [...] van de lidstaten waarbij de vervaardiging, de invoer, de verhandeling of het gebruik van een product [...] wordt verboden"), van richtlijn 2015/1535.

36 De [verwijzende] rechter is evenwel van oordeel dat deze richtlijn in casu niet van toepassing is. Volgens artikel 1, lid 3, van richtlijn 2015/1535 geldt deze richtlijn niet voor regels betreffende zaken die vallen onder een regeling van de Unie inzake telecommunicatiediensten, zoals bedoeld in richtlijn 2002/21. Het staat vast dat richtlijn 2002/21 met ingang van 21 december 2020 is ingetrokken bij artikel 125 van richtlijn 2018/1972 en dat richtlijn 2018/1972 onder meer richtlijn 2002/21 omvat.[16] De litigieuze nationale wettelijke regeling is op 1 februari 2022 in werking getreden en heeft richtlijn 2018/1972 omgezet.

13 Zie arrest van 11 juni 2015, Berlington Hungary e.a. (C-98/14, EU:C:2015:386), punt 87; arrest van de administratieve kamer van de Riigikohus (hoogste rechterlijke instantie) van 27 januari 2010 nr. 3-3-1, punt 15. Te raadplegen via het volgende internetadres: https://www.riigikohus.ee/et/lahendid?asjaNr=3-3-1-79-09.

14 Zie arrest van het Hof van Justitie van 15 november 2016, [redacted] C-268/15, EU:C:2016:874, punt 53.

15 Zie arrest van 28 mei 2020, ECO-WIND Construction, C-727/17, EU:C:2020:393, punten 45 en 46.

16 Zie overweging 4 van richtlijn 2018/1972.

Richtlijn 2018/1972

37 Volgens artikel 1, lid 3, onder c), van richtlijn 2018/1972 doet de richtlijn geen afbreuk aan de acties die door de lidstaten zijn genomen met het oog op de openbare orde, de openbare veiligheid en defensie. Gelet op het feit dat de betrokken nationale regeling ter waarborging van de nationale veiligheid voorziet in beperkingen voor hardware en software in het elektronischecommunicatienetwerk en in een verplichting voor de onderneming om een gebruiksmachtiging aan te vragen, is het onduidelijk of artikel 1, lid 3, onder c), van richtlijn 2018/1972, gelezen in samenhang met artikel 4, lid 2, VEU, aldus moet worden uitgelegd dat het opleggen van dergelijke beperkingen tot de uitsluitende bevoegdheid van de lidstaat behoort en een zuiver nationale maatregel is waarop de bepalingen van richtlijn 2018/1972 niet van toepassing zijn. Een dergelijke uitlegging wordt evenwel in twijfel getrokken door de rechtspraak van het Hof van Justitie volgens welke het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid er niet toe kan leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen.[17] Voor het geval dat artikel 1, lid 3, onder c), van richtlijn 2018/1972 de toepassing van deze richtlijn niet uitsluit, rijst de vraag of de bestreden wettelijke regeling in overeenstemming is met artikel 12, lid 1, van richtlijn 2018/1972.

38 Overeenkomstig artikel 12, lid 1, van richtlijn 2018/1972 waarborgen de lidstaten de vrijheid om, mits aan de door deze richtlijn vastgestelde voorwaarden voldaan is, elektronischecommunicatienetwerken en -diensten aan te bieden. Te dien einde mogen de lidstaten een onderneming niet beletten elektronischecommunicatienetwerken en -diensten aan te bieden, tenzij dat noodzakelijk is om de in artikel 52, lid 1, VWEU vermelde redenen. Elke dergelijke beperking van de vrijheid om elektronischecommunicatienetwerken en -diensten aan te bieden, wordt met redenen omkleed en ter kennis gebracht van de Commissie.

39 Verweerders hebben de Europese Commissie niet in kennis gesteld van de betrokken nationale bepalingen. Gelet op het voorgaande is niet duidelijk of artikel 12, lid 1, van richtlijn 2018/1972 aldus moet worden uitgelegd dat een wettelijke regeling die een communicatieonderneming verplicht om een machtiging aan te vragen voor het gebruik van hardware en software in haar communicatienetwerk, een regeling vormt die een beperking oplegt van de vrijheid om elektronischecommunicatienetwerken en -diensten aan te bieden, die ter kennis moet worden gebracht van de Commissie.[18] Indien dit het geval is, is er in het geval van niet-nakoming van de kennisgevingsplicht geen aanleiding om de

17 Zie arresten van 15 juli 2021, Ministrstvo za obrambo, C-742/19, EU:C:2021:597, punt 40 en de daar aangehaalde rechtspraak, en 16 januari 2024, Österreichische Datenschutzbehörde, C-33/22, EU:C:2024:46, punt 50.

18 Zie arrest ECO-WIND Construction, C-727/17.

betrokken nationale bepalingen op Elisa toe te passen. Evenmin is duidelijk of een dergelijke beperking verenigbaar is met artikel 3, lid 2, onder b), van richtlijn 2018/1972. Het ligt immers voor de hand dat het verbod om de technologie van Huawei in communicatienetwerken te gebruiken, kan leiden tot afhankelijkheid van twee producenten (Nokia en Ericsson). Indien richtlijn 2018/1972 in casu echter niet van toepassing is, gaat het om een wettelijke regeling die binnen de werkingssfeer van artikel 36 VWEU valt.

Artikel 36 VWEU en de algemene beginselen van het Unierecht

40 Iedere handelsregeling van de lidstaten die de intracommunautaire handel al dan niet rechtstreeks, daadwerkelijk of potentieel kan belemmeren, is te beschouwen als een maatregel van gelijke werking als kwantitatieve beperkingen.[19] Volgens de rechter bestaat er geen twijfel over dat er sprake is van een maatregel van gelijke werking als kwantitatieve invoerbeperkingen (artikel 34 VWEU), indien het bestreden besluit van de TTJA Elisa het gebruik van 5G-hardware en -software van Huawei vanaf 1 januari 2026 en van 2G-4G-hardware en -software van Huawei vanaf 1 januari 2030 verbiedt en het goederen betreft die zich in de Unie in het vrije verkeer bevinden.[20] Indien beperkingen gerechtvaardigd zijn uit hoofde van de openbare orde of de openbare veiligheid, bestaat er een uitzondering op het verbod van artikel 34 VWEU (zie artikel 36 VWEU). In het kader van de door de verdragen gewaarborgde fundamentele vrijheden kunnen redenen van openbare orde worden aangevoerd indien er sprake is van een werkelijke, actuele en voldoende ernstige bedreiging van een fundamenteel maatschappelijk belang.[21] In het geval van een dergelijke afwijking van het beginsel van het vrije verkeer van goederen is het aan de nationale autoriteiten om het bewijs te leveren dat de betrokken regeling voldoet aan het evenredigheidsbeginsel.[22]

41 Het staat vast dat de wetgever het doel van de beperking in § 3 ESS heeft omschreven als het waarborgen van de nationale veiligheid. Het begrip „nationale veiligheid” wordt gedefinieerd in de grondslagen van het veiligheidsbeleid die het Riigikogu (parlement) in 2017 heeft vastgesteld,[23] en in het nationale plan voor de ontwikkeling van de defensie 2017-2026 dat door de regering van de Republiek is vastgesteld; in de beginselen van het veiligheidsbeleid wordt het doel van het

19 Arrest van 11 juli 1974, Dassonville, 8/74, EU:C:1974:82, punt 5.

20 In het eveneens bestreden besluit van de KJN is vastgesteld dat Huawei Technologies een van de grootste leveranciers van netwerk- en telecommunicatieapparatuur ter wereld is en in 2018 32 % van de 5G-octrooien in handen had.

21 Arrest van 26 september 2018, [redacted] e.a., C-137/17, EU:C:2018:771, punt 58, en arrest Commissie/Hongarije, C-66/18, punt 181.

22 Zie arresten van 23 oktober 1997, [redacted] C-189/95, EU:C:1997:504, punten 75 en 76, en 5 juni 2007, [redacted] e.a., C-170/04, EU:C:2007:313, punt 50.

23 Elektronisch beschikbaar: https://riigikantselei.ee/jpa.

Estse veiligheidsbeleid omschreven als het waarborgen van de onafhankelijkheid en soevereiniteit van de Estse staat, het voortbestaan van de natie en de staat, de territoriale integriteit, de constitutionele orde en de veiligheid van de bevolking; in het nationale plan voor de ontwikkeling van de defensie wordt het functioneren van de staat en de samenleving in alle omstandigheden omschreven als een van de belangrijkste doelstellingen van de nationale defensie; dit omvat het waarborgen van de continuïteit van kritieke diensten of andere diensten die essentieel zijn voor de nationale defensie; communicatiediensten behoren tot de kritieke diensten, en de aanleg van communicatienetwerken houdt rechtstreeks verband met deze diensten. Daarmee heeft de wetgever de kwestie van de nationale veiligheid ook gekoppeld aan de waarborging van de continuïteit van kritieke diensten, die in de rechtspraak van het Hof onder de openbare veiligheid valt.[24] Ongeacht of er maatregelen worden genomen om de nationale veiligheid of de openbare veiligheid te verzekeren, is de lidstaat echter verplicht om het Unierecht na te leven, met inbegrip van de algemene beginselen ervan.[25] Een van de algemene beginselen van het Unierecht is het evenredigheidsbeginsel.[26] Dit betekent dat zowel de beperking van het vrije verkeer van goederen als de beperking van de vrijheid om elektronischecommunicatienetwerken en -diensten aan te bieden naar behoren gerechtvaardigd en evenredig moeten zijn.

42 In de bestreden voorbereidende administratieve handeling[27] is onderzocht of de in de machtigingsaanvraag vermelde hardware en software van het communicatienetwerk vanwege de fabrikant een bedreiging vormen voor de nationale veiligheid, onder welke voorwaarden de hardware en software van Huawei Technologies Co, Ltd kan worden gebruikt op een wijze die geen bedreiging vormt voor de nationale veiligheid, welke gevolgen een voorwaardelijke machtiging voor Elisa heeft (gelet op de gebruiksduur van de gebruikte technologie en de mogelijkheid om deze te vervangen door die van een andere fabrikant), welke gevolgen de weigering van de machtiging en/of de voorwaardelijke machtiging voor de continuïteit van de communicatiedienst en van de communicatienetwerken, alsook voor de communicatiemarkt en de mededinging, hebben. De verwijzende rechter wenst derhalve te vernemen of de wettelijke regeling van een lidstaat verenigbaar is met artikel 36 VWEU en het evenredigheidsbeginsel die, ter waarborging van de nationale veiligheid, communicatieondernemingen verplichten een machtiging aan te vragen voor het gebruik van hardware en software in hun communicatienetwerk en de

24 Zie arresten Denkavit Futtermittel, 251/78, punt 24; ATRAL, C-14/02, punten 66-69, en Scotch Whisky Association e.a., C-333/14, punt 53.

25 Zie arresten Ministrstvo za obrambo, C-742/19, punt 40 en de daar aangehaalde rechtspraak, alsmede Österreichische Datenschutzbehörde, C-33/22, punt 50.

26 Zie richtlijn 2018/1972, overweging 6; arrest Commissioner of An Garda Síochána e.a., C-140/20, punten 56-59, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 130-132.

27 Besluit van de KJN van 27 oktober 2007.

administratieve autoriteiten niet verplichten om bij de beoordeling van het gevaar van hardware en software met een hoog risico a) na te gaan of de aan de fabrikant verbonden risico's ook gelden voor de specifieke hardware en software, b) de functionaliteit, de locatie en het belang van de specifieke hardware en software te beoordelen in het kader van het aanbieden van een communicatiedienst, en c) te onderzoeken of problemen die verband houden met de staat van vestiging van de fabrikant, ook gelden voor de fabrikant. In het kader van de vaststelling van het gevaar verwijst de rechter naar mededeling C(2023) 4049 def. van de Europese Commissie van 15 juni 2023 „Uitvoering van de EU-toolbox inzake 5G-cyberbeveiliging", waarin de Commissie de besluiten van de lidstaten om Huawei en ZTE te beperken en uit te sluiten gerechtvaardigd en in overeenstemming met de 5G-toolbox[28] achtte. Hoewel de mededeling van de Commissie juridisch niet bindend is voor de lidstaten,[29] is de rechter van oordeel dat het, gelet op de bevoegdheid van de Commissie[30] en het doel van de mededeling, niettemin een nuttig document is voor de beoordeling van de verenigbaarheid van de bestreden beperking met het Unierecht.

Handvest

43 Gelet op artikel 17, lid 1, tweede zin, van het Handvest is het in casu onduidelijk of er sprake is van ontneming van eigendom wanneer een machtiging voor het gebruik van hardware of software die vóór de invoering van de machtigingsverplichting reeds aanwezig was in het communicatienetwerk en actief werd gebruikt, wordt verleend voor een kortere periode dan de gebruiksduur van de hardware of software en de hardware of software rechtmatig werd verworven.

28 Elektronisch beschikbaar: https://digital-strategy.ec.europa.eu/de/library/communication-commission-implementation-5g-cybersecurity-toolbox.

29 Zie artikel 288 VWEU.

30 Zie artikel 17, lid 1, VWEU.