Datum van inontvangstneming	:	15/06/2015

Zaak C-203/15

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:

4 mei 2015

Verwijzende rechter:

Kammarrätten i Stockholm (Zweden)

Datum van de verwijzingsbeslissing:

29 april 2015

Verzoekende partij:

Tele2 Sverige AB

Verwerende partij:

Post- och telestyrelsen

Voorwerp van de procedure in het hoofdgeding

Bevel tot nakoming van de verplichting om verkeersgegevens te bewaren met het oog op wetshandhaving op strafrechtelijk gebied, dat de nationale regelgevende instantie Post- och telestyrelsen (Bestuur Post en Telecommunicatie; hierna: „PTS") heeft gericht aan Tele2 Sverige AB (hierna: „Tele2") op grond van lagen (2003:389) om elektronisk kommunikation (wet [2003:389] betreffende elektronische communicatie; hierna: „LEK").

Voorwerp en rechtsgrondslag van het verzoek om een prejudiciële beslissing

Verzoek om een prejudiciële beslissing overeenkomstig artikel 267 VWEU over de uitlegging van artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van

het Europees Parlement en de Raad van 25 november 2009 (PB L 337, blz. 11), hierna: „richtlijn 2002/58”)

Het verzoek is ingediend in het licht van met name het arrest van het Hof van Justitie van 8 april 2014 in de gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland Ltd e.a. (EU:C:2014:238), waarin het Hof de ongeldigheid vaststelde van richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB L 105, blz. 54) (hierna: „richtlijn 2006/24”).

Het verzoek strekt tot verduidelijking van de vraag of de Zweedse regelgeving inzake gegevensbewaring verenigbaar is met artikel 15, lid 1, van richtlijn 2002/58 alsook de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie en ander Unierecht.

Prejudiciële vragen

„1) Is een algemene verplichting, zoals beschreven [in de punten 1 tot en met 6 infra], om met het oog op wetshandhaving op strafrechtelijk gebied verkeersgegevens te bewaren, welke verplichting zich zonder enig onderscheid, enige beperking of uitzondering uitstrekt tot alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, verenigbaar met artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest van de Grondrechten van de Europese Unie?

2) Indien de eerste vraag ontkennend wordt beantwoord, kan de bewaring dan niettemin toegestaan zijn

a) wanneer de toegang van de nationale instanties tot de gegevens die worden bewaard, is geregeld zoals [beschreven in de punten 7 tot en met 24 infra],

b) wanneer de veiligheidseisen worden geregeld zoals [beschreven in de punten 26 tot en met 31 infra], en

c) alle relevante gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd, en daarna moeten worden gewist, zoals [beschreven in punt 25 infra]?”

Aangehaalde bepalingen van Unierecht

Overweging 11 en artikelen 1, lid 1, 5, lid 1, 6, leden 1 en 2, en 15, lid 1, van richtlijn 2002/58

Artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”)

Aangehaalde bepalingen van nationaal recht

Gezien bovengenoemd doel van het verzoek om een prejudiciële beslissing geeft de verwijzende rechter een gedetailleerde beschrijving van de Zweedse regelgeving inzake gegevensbewaring. De beschrijving is ingedeeld in de volgende vier punten: de omvang van de bewaarplicht, de toegang tot de bewaarde gegevens, de bewaartermijn voor de bewaarde gegevens en de beveiliging van de bewaarde gegevens.

Omvang van de bewaarplicht

1 Richtlijn 2006/24 werd in Zweeds recht omgezet door wijzigingen van de LEK en förordningen (2003:396) om elektronisk kommunikation (besluit [2003:396] betreffende elektronische communicatie; hierna: „FEK”), die in werking traden op 1 mei 2012. De bepalingen over bewaring staan in hoofdstuk 6, §§ 16a tot en met 16f, LEK. §§ 37 tot en met 46 FEK bevatten nadere bepalingen.

2 Uit hoofdstuk 6, § 16a, LEK blijkt dat wie een activiteit uitoefent waarvoor krachtens hoofdstuk 2, §1, van die wet een meldingsplicht bestaat (hierna: „aanbieder”), verplicht is om abonnementsgegevens en andere gegevens over een specifiek elektronisch bericht te bewaren die nodig zijn voor het traceren en identificeren van de bron, de bestemming, de datum, het tijdstip, de duur en de aard van de communicatie, de communicatieapparatuur en de locatie van mobiele communicatieapparatuur bij begin en einde van de communicatie. De verplichting om de gegevens te bewaren heeft betrekking op gegevens die worden gegenereerd of verwerkt bij vaste en mobiele telefoondiensten, het verzenden van berichten, de toegang tot internet en de terbeschikkingstelling van de capaciteit om toegang tot internet te krijgen (aansluiting).

3 De bewaarplicht die aanbieders krachtens Zweeds recht wordt opgelegd, omvat integraal de bewaarplicht die wordt opgelegd bij richtlijn 2006/24. Naast de verplichtingen die werden ingevoerd ter omzetting van richtlijn 2006/24, werd in het Zweedse recht bovendien een verplichting ingevoerd om gegevens te bewaren over mislukte oproepen en de locatie bij het einde van mobiele telefoongesprekken. Overeenkomstig richtlijn 2006/24 strekt de bewaarplicht zich niet uit tot gegevens waaruit de inhoud van de communicatie kan worden opgemaakt.

4 Uit §§ 38 tot en met 43 FEK blijkt meer in het bijzonder welke gegevens dienen te worden bewaard om aan de bewaarplicht van hoofdstuk 6, § 16a, LEK te voldoen.

5 Wat telefoondiensten betreft, dienen onder meer het bellende en opgebelde nummer te worden bewaard, alsook de datum en het traceerbare tijdstip waarop de

communicatie begon en eindigde. Wat mobiele telefoondiensten betreft, blijken bijkomende eisen te gelden. Ook locatiegegevens bij begin en einde van de communicatie moeten bijvoorbeeld worden bewaard. Wat betreft telefoondiensten waarbij internetprotocollen worden gebruikt, moeten behalve het bovengenoemde onder meer ook de IP-adressen van de beller en de opgebelde persoon worden bewaard. Voor het verzenden van berichten geldt onder meer dat het nummer, IP-adres of ander berichtadres van verzenders en ontvangers moet worden bewaard. Wat de toegang tot internet betreft, moet bijvoorbeeld het IP-adres van de gebruiker worden bewaard, alsook de datum en het traceerbare tijdstip van de log-in en log-off van de internetsessie.

6 Uit hoofdstuk 6, § 16c, LEK blijkt dat gegevens die op grond van § 16a worden bewaard, uitsluitend mogen worden verwerkt om te worden verstrekt overeenkomstig § 22, eerste alinea, punt 2, LEK, hoofdstuk 27, § 19, van rättegångsbalken (1942:[740]) (gerechtelijk wetboek [1942:470]; hierna: „RB") of lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (wet [2012:278] betreffende de verzameling van gegevens over elektronische communicatie bij de inlichtingsactiviteiten van de met misdaadbestrijding belaste instanties; hierna: „wet gegevensverzameling").

Toegang tot de bewaarde gegevens

7 De toegang tot de bewaarde gegevens wordt hoofdzakelijk geregeld door drie Zweedse wetten, namelijk de LEK, de RB en de wet gegevensverzameling.

LEK

8 Uit hoofdstuk 6, § 22, eerste alinea, punt 2, LEK blijkt dat een aanbieder desgevraagd abonnementsgegevens moet verstrekken aan het openbaar ministerie, de politie, de inlichtingendienst of een andere instantie die tot taak heeft op te treden tegen strafbare feiten, indien de gegevens verband houden met de verdenking van een strafbaar feit. Op grond van de bepaling wordt niet vereist dat sprake is van een ernstig strafbaar feit.

9 Met abonnementsgegevens worden met name gegevens bedoeld over naam, titel, adres, nummer en IP-adres.

10 Het verstrekken van abonnementsgegevens op grond van de LEK vereist geen voorafgaande controle. Nadat gegevens zijn verstrekt, kunnen Datainspektionen (toezichthouder inzake gegevensverwerking) en Säkerhets- och integritetsskyddsnämnden (commissie voor de bescherming van de veiligheid en de persoonlijke levenssfeer) toezicht uitoefenen op de naleving door de instanties van de voorschriften inzake de verwerking van persoonsgegevens. Daarnaast oefenen Riksdagens ombudsmän (Justitieombudsmannen [JO], ombudsdienst van het parlement) en Justitiekanslern (JK, kanselier van justitie) toezicht uit op de bestuursorganen van de staat. Het toezicht op de naleving van de LEK door de

aanbieders wordt uitgeoefend door de PTS. De kring van overheidspersonen die toegang kunnen krijgen tot de gegevens, is niet beperkt.

RB

11 In de RB wordt geregeld in welke gevallen overheidsinstanties in gerechtelijke onderzoeken gegevens over elektronische communicatie mogen verzamelen.

12 Uit hoofdstuk 27, § 19, RB blijkt dat geheim toezicht op elektronische communicatie in de regel is toegestaan bij gerechtelijke onderzoeken inzake (1) strafbare feiten waarop ten minste zes maanden gevangenisstraf staat, (2) strafbare feiten als bedoeld in hoofdstuk 4, § 9c, brottsbalken (wetboek van strafrecht) (computerkraak), strafbare feiten als bedoeld in hoofdstuk 16, § 10a, brottsbalken die niet als gering zijn te beschouwen (strafbare feiten op het gebied van kinderpornografie), strafbare feiten als bedoeld in § 1 narkotikastrafflagen (1968:64) (strafwet [1968:64] inzake verdovende middelen), strafbare feiten als bedoeld in § 6, eerste alinea, van lagen (2000:1225) om straff för smuggling (wet [2000:1225] ter bestraffing van smokkel), dan wel (3) poging tot, voorbereiding van of samenspanning tot strafbare feiten als bedoeld onder 1 of 2, indien op een dergelijke handeling straf is gesteld.

13 Voorts blijkt uit hoofdstuk 27, § 19, RB dat onder geheim toezicht op elektronische communicatie wordt verstaan dat in het geheim gegevens worden verzameld over (1) berichten die in een elektronisch communicatienetwerk worden overgebracht of zijn overgebracht naar of van een telefoonnummer of ander adres, (2) de elektronische communicatieapparatuur die in een bepaald geografisch gebied aanwezig was, of (3) het geografische gebied waarin bepaalde elektronische communicatieapparatuur aanwezig is of was.

14 Gegevens over de inhoud van berichten kunnen op grond van hoofdstuk 27, §19 RB niet worden verzameld.

15 Uit hoofdstuk 27, §20 RB blijkt dat geheim toezicht op elektronische communicatie in de regel enkel is toegestaan wanneer iemand op redelijke gronden van het strafbare feit wordt verdacht en de maatregel van bijzonder belang is voor het onderzoek. De maatregel mag enkel betrekking hebben op (1) een telefoonnummer of ander adres dan wel bepaalde elektronische communicatieapparatuur die in de periode waarvoor de toestemming geldt, in het bezit van de verdachte is of geweest is dan wel waarvan anderszins kan worden aangenomen dat zij door de verdachte is gebruikt of zal worden gebruikt, of (2) een telefoonnummer of ander adres dan wel bepaalde elektronische communicatieapparatuur ten aanzien waarvan bijzondere redenen bestaan om aan te nemen dat de verdachte in de periode waarvoor de toestemming geldt, daarmee contact heeft opgenomen of zal opnemen.

16 Geheim toezicht op elektronische communicatie is daarnaast toegestaan om te onderzoeken wie redelijkerwijs kan worden verdacht van het strafbare feit,

wanneer de maatregel van bijzonder belang is voor het onderzoek. Alleen wanneer het toezicht betrekking heeft op het verleden, mogen daarbij gegevens worden verzameld over berichten. Dergelijk geheim toezicht is volgens hoofdstuk 27, § 19, vierde alinea, RB enkel toegestaan bij een gerechtelijk onderzoek inzake een strafbaar feit dat op grond van § 18, tweede alinea, aanleiding kan geven tot het heim afluisteren van elektronische communicatie, dat wil zeggen wanneer het gerechtelijk onderzoek betrekking heeft op (1) een strafbaar feit waarop ten minste twee jaar gevangenisstraf staat, (2) poging tot, voorbereiding van of samenspanning tot een dergelijk strafbaar feit, dan wel (3) een ander strafbaar feit, indien gelet op de omstandigheden kan worden aangenomen dat ter zake van dat feit een straf zal worden uitgesproken die twee jaar gevangenisstraf te boven gaat.

17 Ingevolge hoofdstuk 27, § 21, RB worden kwesties inzake geheim toezicht op elektronische communicatie in de regel getoetst door de rechter op verzoek van de openbare aanklager.

18 Indien te vrezen valt dat het verkrijgen van rechterlijke toestemming voor geheim toezicht op elektronische communicatie een vertraging of ander nadeel met zich mee zou brengen die onderscheidenlijk dat van wezenlijk belang is voor het onderzoek, mag de toestemming voor de maatregel worden gegeven door de openbare aanklager in afwachting van de beslissing van de rechter. In dergelijke gevallen moet de openbare aanklager de rechter onverwijld schriftelijk van de maatregel in kennis stellen. De rechter moet vervolgens ten spoedigste onderzoeken of de maatregel gewettigd is (zie hoofdstuk 27, § 21a, RB).

Wet gegevensverzameling

19 Volgens § 1 van de wet gegevensverzameling mogen de politie, de inlichtingendienst of de douane onder de in de wet gestelde voorwaarden in de uitoefening van hun inlichtingsactiviteiten in het geheim bij degene die volgens de LEK een elektronisch communicatienetwerk of een elektronische communicatiedienst aanbiedt, gegevens verzamelen over (1) berichten die in een elektronisch communicatienetwerk zijn overgebracht naar of van een telefoonnummer of ander adres, (2) de elektronische communicatieapparatuur die in een bepaald geografisch gebied aanwezig was, of (3) het geografische gebied waarin bepaalde elektronische communicatieapparatuur aanwezig is of was.

20 De gegevens mogen volgens §§ 2 en 3 van de wet gegevensverzameling worden verzameld indien de omstandigheden van dien aard zijn dat de maatregel van bijzonder belang is ter voorkoming, verhindering of ontdekking van strafbare activiteiten die strafbare feiten behelzen waarop ten minste twee jaar gevangenisstraf staat of die deel uitmaken van de opsomming in § 3 (onder meer verschillende vormen van sabotage en spionage). De redenen voor de maatregel moeten in dat geval opwegen tegen de aantasting of overige ongemakken als gevolg van de maatregel voor degene tegen wie de maatregel is gericht of enig ander met de maatregel strijdig belang.

21 Het besluit om gegevens te verzamelen wordt genomen door het hoofd van de betrokken overheidsinstantie of een andere ambtenaar aan wie het hoofd het beslissingsrecht delegeert. Delegatie veronderstelt dat die ambtenaar de specifieke bekwaamheid, opleiding en ervaring heeft die nodig is (§ 4 van de wet gegevensverzameling).

22 In de besluiten dient te worden vermeld op welke strafbare activiteit en op welke periode het betreffende besluit ziet, alsook op welk telefoonnummer of ander adres, op welke elektronische communicatieapparatuur of op welk geografisch gebied het besluit betrekking heeft. De periode waarvoor het besluit geldt, mag niet langer zijn dan noodzakelijk en mag, wanneer die periode na het besluit valt, niet meer dan een maand bedragen (§ 5 van de wet gegevensverzameling).

23 De verzameling van gegevens vereist geen voorafgaande controle. Säkerhets- och integritetsskyddsnämnden dient evenwel krachtens § 6 van de wet gegevensverzameling in kennis te worden gesteld van elk besluit over het verzamelen van gegevens. Op grond van § 1 van lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (wet [2007:980] betreffende het toezicht op bepaalde activiteiten tot misdaadbestrijding) oefent Säkerhets- och integritetsskyddsnämnden toezicht uit op de toepassing van de wet door de instanties die met misdaadbestrijding zijn belast.

24 Krachtens § 8 van de wet gegevensverzameling is toestemming vereist om verzamelde gegevens in een gerechtelijk onderzoek te gebruiken. Het ontbreken van toestemming voor geheim toezicht op elektronische communicatie staat er niet aan in de weg dat de verzamelde gegevens ten grondslag liggen aan een besluit tot inleiding van een gerechtelijk onderzoek. Nadat een gerechtelijk onderzoek is ingeleid, mogen verzamelde gegevens in dat onderzoek evenwel enkel worden gebruikt als de rechter toestemming heeft verleend voor geheim toezicht op elektronisch communicatie als bedoeld in hoofdstuk 27, § 19, RB. Indien toestemming wordt verleend, staat het aan de openbare aanklager te beslissen of de gegevens opnieuw bij de operatoren moeten worden opgevraagd dan wel of de gegevens die bij de inlichtingsactiviteiten zijn verkregen, moeten worden overgedragen naar het gerechtelijk onderzoek.

Bewaartermijn voor de bewaarde gegevens

25 Uit hoofdstuk 6, § 16d, LEK blijkt dat gegevens als bedoeld in hoofdstuk 6, § 16a, LEK moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd. Daarna moeten de gegevens onverwijld worden gewist, tenzij in de tweede alinea anders is bepaald. Wanneer vóór ommekomst van de bewaartermijn gegevens zijn opgevraagd, doch nog niet verstrekt, moeten zij volgens hoofdstuk 6, § 16d, tweede alinea, LEK onverwijld worden gewist nadat zij zijn verstrekt.

Beveiliging van de bewaarde gegevens

26 Ingevolge hoofdstuk 6, § 20, LEK mag wie in verband met de terbeschikkingstelling van een elektronisch communicatienetwerk of een elektronische communicatiedienst bekend is geworden met of toegang heeft gekregen tot (1) een abonnementsgegeven, (2) de inhoud van een elektronisch bericht of (3) een ander gegeven met betrekking tot een specifiek elektronisch bericht, datgene waarmee hij bekend is geworden of waartoe hij toegang heeft gekregen, niet onbevoegdelijk doorgeven of benutten. Die geheimhoudingsplicht geldt niet ten opzichte van degene die betrokken was bij de uitwisseling van een elektronisch bericht dan wel anderszins een dergelijk bericht heeft verzonden of ontvangen. De geheimhoudingsplicht inzake gegevens als bedoeld in de eerste alinea, punten 1 en 3, geldt evenmin ten opzichte van de houder van een abonnement dat is gebruikt voor een elektronisch bericht.

27 Uit hoofdstuk 6, § 3a, LEK volgt dat aanbieders waarvoor de bewaarplicht geldt, de specifieke technische en organisatorische maatregelen moeten treffen die nodig zijn om de bewaarde gegevens bij de verwerking ervan te beschermen. Blijkens de ontstaansgeschiedenis van die bepaling wordt geen ruimte toegestaan om bij het bepalen van het beveiligingsniveau een afweging te maken tussen techniek, kosten en het risico op een schending van de persoonlijke levenssfeer (wetsvoorstel 2010/11:46, blz. 75).

28 Nadere voorschriften over de beveiliging van de gegevens zijn neergelegd in § 37 FEK en in Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål (PTSFS 2012:4) (voorschriften en algemene richtsnoeren van PTS inzake beschermingsmaatregelen in verband met de bewaring en overige verwerking van gegevens met het oog op misdaadbestrijding [PTSFS 2012:4]). Uit die voorschriften blijkt onder meer dat aanbieders maatregelen dienen te nemen om de gegevens te beschermen tegen onopzettelijke of ongeoorloofde vernietiging, tegen de ongeoorloofde bewaring en verwerking van of toegang tot de gegevens, alsook tegen de ongeoorloofde openbaarmaking ervan. De aanbieder moet tevens voortdurend en stelselmatig zorg besteden aan de beveiliging in het licht van de bijzondere risico's die de bewaarplicht met zich meebrengt.

29 In het Zweedse recht ontbreken bepalingen over de plaats waar de gegevens dienen te worden bewaard.

30 Ingevolge hoofdstuk 7, § 1, LEK oefent de toezichthoudende autoriteit toezicht uit op de naleving van de wet alsook op de naleving van de besluiten over plichten of voorwaarden en van de voorschriften die krachtens de wet zijn vastgesteld. De toezichthoudende autoriteit oefent eveneens toezicht uit op de naleving van de uitvoeringsmaatregelen als bedoeld in onder meer artikel 4, lid 5, van richtlijn 2002/58.

31 Krachtens hoofdstuk 7, § 3, LEK is de toezichthoudende autoriteit bevoegd een aanbieder te gelasten aan de autoriteit inlichtingen en documenten te verstrekken die nodig zijn voor het toezicht op de naleving. Indien de toezichthoudende autoriteit redenen vindt om te vermoeden dat wie een activiteit als bedoeld in de LEK uitoefent, inbreuk maakt op de wet of de krachtens de wet vastgestelde voorschriften of een uitvoeringsmaatregel als bedoeld in hoofdstuk 7, § 1, LEK, stelt de autoriteit degene die de activiteit uitoefent daarvan in kennis en biedt zij hem de mogelijkheid binnen een redelijke termijn opmerkingen te maken (zie hoofdstuk 7, § 4, LEK). De toezichthoudende autoriteit is bevoegd de nodige bevelen en verboden uit te vaardigen opdat onmiddellijk of binnen een redelijke termijn een einde wordt gemaakt aan een overtreding als bedoeld in hoofdstuk 7, § 4, LEK. Een dergelijk bevel of verbod kan worden versterkt met een dwangsom. Indien het bevel niet wordt opgevolgd, is de toezichthoudende autoriteit bevoegd te besluiten dat wie een verplichting niet is nagekomen de activiteit geheel of gedeeltelijk moet staken (zie hoofdstuk 7, § 5, LEK).

Korte uiteenzetting van de feiten en de procedure in het hoofdgeding

32 De dag nadat het Hof van Justitie van de Europese Unie het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238) had gewezen, dat wil zeggen op 9 april 2014, deed Tele2 PTS een schrijven toekomen waarin Tele2 onder meer meedeelde dat de onderneming met ingang van 14 april 2014 niet langer gegevens zou bewaren overeenkomstig hoofdstuk 6 van de LEK. Tele2 zou tevens de gegevens wissen die eerder waren bewaard overeenkomstig hoofdstuk 6 van de LEK. De reden was dat Tele2 na een analyse had geconstateerd dat de eisen in de Zweedse wetgeving ter omzetting van richtlijn 2006/24 niet in overeenstemming waren met het Handvest. Bijgevolg was de onderneming van mening dat de Zweedse eisen inzake gegevensbewaring in strijd waren met het Unierecht zodat de Zweedse telecommunicatieoperatoren ze buiten toepassing moesten laten.

33 Kort daarop deelde Rikspolisstyrelsen (rijkspolitiebestuur) PTS in een schrijven mee dat de weigering van PTS om overeenkomstig de vigerende wetgeving met het oog op misdaadbestrijding verkeersgegevens te verstrekken, grote gevolgen heeft voor de activiteiten van de politie tot misdaadbestrijding.

34 Op 29 april 2014 benoemde de regering een bijzondere onderzoeker die de taak kreeg de toepasselijkheid van de Zweedse regels te onderzoeken in het licht van het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238). De onderzoeker diende een eerste verslag in op 13 juni 2014 en kwam daarin tot de algemene conclusie dat de Zweedse regelgeving inzake gegevensbewaring overeenkomstig hoofdstuk 6, §§ 16a tot en met 16f, LEK niet in strijd was met het Unierecht of het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: „EVRM”).

35 Bij besluit van 27 juni 2014 richtte PTS een bevel aan Tele2 om uiterlijk op 25 juli 2014 overeenkomstig hoofdstuk 6, § 16a, LEK juncto §§ 37 tot en met 43 FEK gegevens te bewaren.

36 Tele2 stelde tegen het besluit van PTS beroep in bij Förvaltningsrätten i Stockholm (bestuursrechtbank te Stockholm). Förvaltningsrätten verwierp het beroep bij vonnis van 13 oktober 2014. Het oordeelde dat de Zweedse bepalingen inzake gegevensbewaring vallen onder de door artikel 15, lid 1, van richtlijn 2002/58 geboden mogelijkheid om nationale wettelijke maatregelen te treffen ter beperking van de omvang van bepaalde in de richtlijn bedoelde rechten en plichten. Förvaltningsrätten onderstreepte in het bijzonder dat het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238) aldus dient te worden begrepen dat richtlijn 2006/24 ongeldig is verklaard omdat de geconstateerde tekortkomingen van de richtlijn, *in hun geheel beschouwd*, impliceren dat de richtlijn niet voldoet aan het Unierechtelijke vereiste van evenredigheid van beperkingen van de rechten en vrijheden.

37 Tele2 heeft tegen het vonnis van förvaltningsrätten hoger beroep ingesteld en vordert dat kammarrätten (bestuursrechter in hoger beroep) dat vonnis hervormt alsook het litigieuze bevel nietig verklaart.

38 PTS concludeert tot verwerping van het hoger beroep.

Voornaamste argumenten van partijen in het hoofdgeding

39 Tele2 stelt zich op het standpunt dat de bepalingen over gegevensbewaring van hoofdstuk 6 van de LEK, evenals richtlijn 2006/24, in strijd zijn met het EVRM en bijgevolg ook met de Zweedse grondwet. PTS was daarom rechtens niet bevoegd om die bepalingen toe te passen en te handhaven door Tele2 te gelasten de gegevensbewaring te hervatten.

40 Tele2 is voorts van mening dat de omvang van de bewaarplicht reeds op zichzelf onevenredig is. Om te kunnen beoordelen of de Zweedse bewaarplicht verder gaat dan wat noodzakelijk is, dient een beoordeling te worden verricht van elke afzonderlijke in de §§ 38 tot en met 43 FEK neergelegde soort bewaarplicht en te worden nagegaan of elk van die verplichtingen een noodzakelijke beperking op de fundamentele rechten en vrijheden vormt. De onderneming verwerpt het argument dat een alomvattende beoordeling moet worden verricht om uit te maken of de Zweedse bepalingen inzake gegevensbewaring voldoen aan het evenredigheidsvereiste, waarbij de omvang van de bewaarplicht wordt beschouwd in het licht van de wijze waarop de bepalingen over de toegang tot de gegevens zijn geformuleerd, de duur van de bewaartermijn voor de gegevens en de beveiliging van de bewaarde gegevens.

41 Het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238) kan volgens Tele2 niet aldus worden uitgelegd dat de aantasting van de fundamentele rechten en

vrijheden die wordt gevormd door de ruime verplichting om gegevens te bewaren, kan worden „verholpen” door de toegang tot de bewaarde gegevens te beperken.

42 Tele2 wenst tevens de aandacht te vestigen op de volgende ernstige tekortkomingen van de Zweedse bepalingen:

> De toegang tot de bewaarde gegevens op grond van de LEK vereist niet dat de gegevens verband houden met de verdenking van ernstige strafbare feiten.
>
> Meerdere overheidsinstanties kunnen toegang krijgen tot de gegevens, zonder dat een voorafgaande controle door een rechter of onafhankelijke overheidsinstantie plaatsvindt.
>
> De kring van overheidspersonen die toegang kunnen krijgen tot de gegevens, is niet beperkt.
>
> Het verzamelen van gegevens vindt plaats zonder enige voorafgaande controle.
>
> Er bestaat geen verbod op de doorgifte van gegevens buiten de EU.

43 PTS voert aan dat het feit dat het Hof van Justitie van de Europese Unie richtlijn 2006/24 ongeldig heeft bevonden, niet automatisch impliceert dat ook de Zweedse wetgeving ongeldig is. Ook al bestaat er niet langer een Unierechtelijke verplichting voor de lidstaten om verkeersgegevens te bewaren met het oog op wetshandhaving op strafrechtelijk gebied, het Unierecht staat toe dat een dergelijke bewaring plaatsvindt zolang is voldaan aan de eisen van richtlijn 2002/58 en het overige Unierecht.

44 Op basis van een alomvattende beoordeling is PTS van mening dat er geen redenen zijn om de Zweedse bepalingen niet toe te passen en dat Tele2 bijgevolg gehouden is haar verplichting krachtens hoofdstuk 6, § 16a, LEK na te komen.

Korte uiteenzetting van de motivering van de verwijzing

45 Kammarrätten is net als PTS van oordeel dat het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238) de mogelijkheid om verkeersgegevens te bewaren onverlet laat, zolang is voldaan aan de eisen van richtlijn 2002/58 en het Unierecht ook overigens niet wordt geschonden.

46 Het Hof van Justitie van de Europese Unie stelde in het bovengenoemde arrest vast dat de bewaring van verkeersgegevens geschikt was om het met richtlijn 2006/24 nagestreefde doel te bereiken, aangezien het tot wetshandhaving op strafrechtelijk gebied nuttig was toegang te krijgen tot gegevens van de soort als aan de orde. Opdat de bewaring ook een evenredige maatregel zou zijn om

strafbare feiten te bestrijden, moest de beperking van de fundamentele vrijheden naar het oordeel van het Hof worden beperkt tot wat *strikt noodzakelijk* is. Daaruit werd de conclusie getrokken dat de Unieregeling duidelijke en precieze regels betreffende de draagwijdte en toepassing van de betrokken maatregel moet bevatten die minimale eisen stellen om een doeltreffende bescherming mogelijk te maken tegen het risico op misbruik, onrechtmatige raadpleging en onrechtmatig gebruik van persoonsgegevens van particulieren. Derhalve moeten aan nationale bepalingen dezelfde eisen worden gesteld. Het Hof vestigde in zijn evenredigheidstoetsing voorts de aandacht op een aantal specifieke kwesties.

47 Het Hof stelde in de punten 56 tot en met 59 van zijn arrest vast dat de omvang van de bewaarplicht krachtens de artikelen 3 en 5 van richtlijn 2006/24 inhield dat verkeersgegevens moesten worden bewaard met betrekking tot alle personen en alle elektronische communicatiemiddelen, zonder dat enig onderscheid werd gemaakt naargelang de gegevens relevant zouden kunnen zijn ter verwezenlijking van de doelstelling om zware criminaliteit te bestrijden. Die richtlijn strekte zich uit tot alle elektronische communicatiemiddelen, waarvan het gebruik wijdverspreid is en die een steeds grotere plaats innemen in het dagelijkse leven. Bovendien gold zij voor alle abonnees en geregistreerde gebruikers. Zij leidde dus tot een aantasting van de fundamentele rechten van bijna de gehele Europese bevolking. De bewaarplicht strekte zich uit tot personen die er niet van werden verdacht enige band te hebben met zware criminaliteit, zonder dat zelfs maar in een uitzondering werd voorzien voor de beroepscategorieën waarvan de communicatie volgens nationale bepalingen onder een geheimhoudingsplicht valt. Evenmin bevatte de richtlijn beperkingen in tijd of ruimte en/of beperkingen tot een bepaalde groep mensen waardoor de bewaarplicht enkel zou gelden voor gegevens die om de een of andere reden kunnen worden geacht van belang te zijn om ernstige strafbare feiten te voorkomen, te onderzoeken of te vervolgen.

48 Het Hof van Justitie van de Europese Unie bekritiseerde op een aantal punten dat de richtlijn de toegang tot de te bewaren gegevens niet nader regelde, maar het in grote mate aan de lidstaten overliet zelf die kwestie te regelen (punten 60 tot en met 62 van het arrest). Het Hof merkte op dat er geen objectief criterium bestond dat de toegang tot gegevens beperkte naargelang van de ernst van het strafbare feit. In de richtlijn werd evenmin nader geregeld hoe de nationale instanties toegang zouden moeten krijgen tot de gegevens. Verder bevatte de richtlijn geen bepalingen die het aantal personen dat toegang kon krijgen tot de gegevens, beperkten tot wat absoluut noodzakelijk kon worden geacht. Het Hof beklemtoonde eveneens dat de toegang van de nationale instanties tot bewaarde verkeersgegevens niet afhankelijk was gemaakt van een voorafgaande controle door een rechter of een ander orgaan dat tot taak had de toegang te beperken tot wat strikt noodzakelijk kan worden geacht.

49 Kammarrätten is van oordeel dat er zowel argumenten zijn voor als tegen de opvatting dat de ruime bewaarplicht die wordt opgelegd door hoofdstuk 6, § 16a, LEK, verenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, de artikelen 7, 8

en 52, lid 1, van het Handvest en ander Unierecht. Tele2 en PTS verschillen van mening over de wijze waarop het arrest Digital Rights Ireland Ltd e.a. (EU:C:2014:238) dient te worden uitgelegd, en kammarrätten wenst daarom een eenduidig antwoord te krijgen op de vraag of het Hof van Justitie van de Europese Unie in dat arrest een afgewogen beoordeling heeft verricht van de omvang van de bewaarplicht en de bepalingen inzake de toegang tot de gegevens, de bewaartermijn en de beveiliging.