THOMAS
DOESBURG
POPPELAARS
STRAFRECHTADVOCATEN

mr. Erik Thomas
mr. Adam Doesburg
mr. ing. Ruben Poppelaars

t. 0763030520
f. 0763030521
info@tdpadvocaten.nl
www.tdpadvocaten.nl
Chassésingel 4
4811 HA Breda

STANDPUNT EN VERZOEK OM PREJUDICIËLE VRAGEN, IN VERBAND MET HET BEWAREN EN GEBRUIK VAN ENCROCHATDATA.

ONDERZOEK FINLAND.

mr. ing. R.B.M. Poppelaars

5 februari 2021

Inhoud

Op alle werkzaamheden van TDP advocaten zijn algemene voorwaarden van toepassing. In deze voorwaarden is onder meer opgenomen dat alle aansprakelijkheid is beperkt tot het bedrag in het betreffende geval onder de aansprakelijkheidsverzekering wordt uitbetaald. De voorwaarden zijn geplaatst op www.tdpadvocaten.nl. TDP advocaten bestaat uit verschillende rechtspersonen, is gevestigd in Breda en is ingeschreven bij de KvK te Breda onder nummer 81238630.

Inleiding.

Dit stuk beschrijft de visie van de verdediging in de zaak ‘Finland’, op de rechtmatigheid van het bewaren en gebruiken van de Encrochatdata, wat in deze zaak heeft geleid tot belastend bewijs jegens cliënt. In verband met dit standpunt wordt voorts voorgesteld om prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie (nader te noemen: het Hof). Het standpunt van de verdediging is namelijk dat het gebruik van de Encrochatdata zoals hier is gebeurd, en overigens ook nog gebeurt, in strijd is met het Unierecht.

Inmiddels zijn er een aantal beslissingen van rechtbanken op onderzoekswensen gepubliceerd, waarin ook overwegingen zijn gewijd aan het Unierechtelijk perspectief dat hier ter sprake komt. In de visie van de verdediging hebben de rechtbanken in die cases het Unierecht onjuist geïnterpreteerd. Gelet op de complexiteit van het ter zake doende Unierecht, wordt een uitgebreide beschouwing gegeven van de jurisprudentie die in de visie van de verdediging relevant is.

Daarna wordt ingegaan op de vraag of het gebruik van de Encrochatdata, dat heeft geleid tot de informatie die het bewijs tegen cliënt vormt in onderhavige zaak, valt binnen de werkingssfeer van het Unierecht en zo ja, wat de ter zake doende regelgeving dan is.

Dan wordt ingegaan op het standpunt van het OM, inhoudende dat het gebruik van de data heeft plaatsgevonden in een ander voorbereidend onderzoek, waardoor de rechtmatigheid van dat gebruik geen onderdeel uitmaakt van de toets die uw rechtbank in de onderhavige zaak dient aan te leggen. In de visie van de verdediging is die visie namelijk ook in strijd met het Europees recht, meer specifiek met het recht op een effectief rechtsmiddel. Voorts zal worden beargumenteerd waarom de beoordeling van de rechtmatigheid van de Encrochatdata van belang is voor de beoordeling van de vragen van art. 348 en 350 Sv.

Na te hebben geconcludeerd dat het gebruik van de Encrochatdata valt binnen de werkingssfeer van het Unierecht en de beoordeling van de rechtmatigheid van belang is voor de beantwoording van de vragen van art. 348 en 350 Sv, zal worden beargumenteerd waarom het gebruik van de Encrochatdata in strijd is met het Unierecht.

Tot slot wordt beargumenteerd waarom in de visie van de verdediging prejudiciële vragen aan het Hof van Justitie van de Europese Unie dienen te worden gesteld, waarbij ook wordt ingegaan op het juridisch kader die de rechtbank dient te hanteren bij een verzoek tot het stellen van prejudiciële vragen.

Ontwikkeling Unierechtelijke jurisprudentie.

Tijdens verschillende zittingen in verschillende zaken is door de verdediging van verscheidene verdachten reeds geopperd dat het gebruik van de Encrochatdata in strijd is met hetgeen het Hof van Justitie op 6 oktober 2020 heeft overwogen, in een tweetal arresten. Ook de verdediging in onderhavige zaak stelt zich op dat standpunt. Een enkele blik op die twee arresten geeft echter onvoldoende inzicht in de ontwikkeling van het Unierecht in dit kader. Om daar wel voldoende inzicht in te hebben, is een beschouwing van eerdere jurisprudentie onontbeerlijk.

Digital Rights, 8 februari 2014 (ECLI:EU:C:2014:238).

Het eerste relevante arrest is het Digital Rights-arrest. Enige bespreking van de achtergrond is hiervoor relevant.

Achtergrond.

Dit arrest gaat over de compatibiliteit van richtlijn 2006/24, met het Handvest van de Grondrechten van de Europese Unie (verder: het Handvest). Deze richtlijn betreft het bewaren van gegevens door aanbieders van elektronische communicatiediensten. Met die richtlijn wordt ook richtlijn 2002/58 gewijzigd. Die richtlijn betreft de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

In richtlijn 2002/58 is in art. 5 lid 1 beschreven dat lidstaten middels nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten garanderen. Uitzondering op die vertrouwelijkheid is de technische opslag die nodig is voor het overbrengen van de informatie, alsmede een wettelijke grondslag op basis van art. 15 lid 1 van die richtlijn.

Art. 15 lid 1 van deze richtlijn beschrijft dat wettelijke maatregelen kunnen worden getroffen ter beperking van de reikwijdte van art. 5, maar ook andere artikelen uit die richtlijn, wanneer die in een democratische samenleving, redelijk en proportioneel zijn ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, of van onbevoegd gebruik van het elektronische communicatiesysteem.

Waar vertrouwelijkheid in richtlijn 2002/58 het uitgangspunt is, is het uitgangspunt in richtlijn 2006/24 de opslag van gegevens. In art. 5 van deze richtlijn wordt een groot aantal gegevens benoemd dat dient te worden opgeslagen, zoals – maar zeker niet beperkt tot – telefoonnummers van gebruikers en ontvangers, IP-adressen en locatiegegevens. Ook creëerde deze richtlijn de mogelijkheid voor wettelijke bepalingen op basis waarvan nationale autoriteiten toegang kregen tot deze opgeslagen gegevens.

Standpunten ten grondslag aan de prejudiciële vragen.

Tegen de verbindendheid van richtlijn 2006/24 is de Ierse organisatie Digital Rights aldaar een procedure gestart. Het standpunt dat zij innamen, was dat deze richtlijn en de implementatiewetgeving ongeldig diende te worden verklaard, omdat het in strijd zou zijn met het evenredigheidsbeginsel ex. art. 5 lid 4 van het Verdrag betreffende de EU (VEU), art. 21 van het Verdrag betreffende de werking van de EU (Art. 21 VWEU) en de artikelen 7, 8, 11 en 41 van het Handvest. Deze artikelen betreffen de rechten op privéleven, bescherming van persoonsgegevens, vrijheid van meningsuiting en behoorlijk bestuur.

Ook in Oostenrijk werd er geprocedeerd tegen de verbindendheid van de voornoemde richtlijn. Daarbij werd ook gerefereerd aan voornoemde artikelen, alsmede aan art. 52 van het Handvest.

Overwegingen Hof van Justitie EU.

Inbreuk?

Over de inhoud van de artikelen die de verplichting van bewaring voorschrijven, overwoog het Hof:

> *"uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren."1*

Het Hof komt tot de conclusie dat de bewaarplicht rechtstreeks en specifiek het privéleven en dus de gewaarborgde rechten in art. 7 Handvest raakt. Ook art. 8 Handvest wordt rechtstreeks geraakt. In verband met de vrijheid van meningsuiting ex art. 11 Handvest, overweegt het Hof dat niet is uitgesloten dat de combinatie van de bewaarde gegevens, een beeld geven van de wijze waarop zij hun communicatiemiddelen gebruiken en aldus een beeld geven van de wijze waarop zij hun vrijheid van meningsuiting effectueren. Het bewaren van de gegevens kan dus een inbreuk maken op art. 11 Handvest. In dit arrest wordt hier niet verder op ingegaan, omdat de overwegingen in verband met art. 7 en 8 Handvest voldoende zijn voor de uiteindelijke conclusie.

De inmenging op voornoemde grondrechten door de artikelen van de richtlijn wordt allereerst gevormd door de verplichting aan elektronische communicatiediensten om de data te bewaren. Vervolgens vormt de toegang van de nationale autoriteiten tot die gegevens ook weer een inbreuk in de betreffende rechten. Het overweegt voorts:

> *"Vastgesteld moet worden dat richtlijn 2006/24 een **zeer ruime en bijzonder zware inmenging** vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele rechten, zoals de advocaat-generaal met name in de punten 77 en 80 van zijn conclusie heeft opgemerkt. Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of geregistreerde gebruiker hierover wordt ingelicht, **bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden**, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt."2*

Inbreuk gerechtvaardigd?

Het hof gaat in op de vraag of de inbreuk is gerechtvaardigd. Daarbij slaat hij acht op art. 52 Handvest. Indien grondrechten worden beperkt, dienen die beperkingen bij wet te worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. *"Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen."*, zo overweegt het Hof.

---

1 Par. 27.
2 Par. 37.

Het Hof stelt vervolgens vast dat het doel van de inbreuk is bij te dragen aan de bestrijding van ernstige criminaliteit, en daarmee aan de openbare veiligheid. Het betreft dus daadwerkelijk een door de Unie erkende doelstelling. De vervolgvraag is dan of dit ook evenredig is. Onder verwijzing naar eerdere uitspraken, overweegt het hof dat eraan *"zij herinnerd dat het evenredigheidsbeginsel […] vereist dat handelingen van de instellingen van de Unie geschikt zijn om de door de betrokken regeling nagestreefde legitieme doelstellingen te verwezenlijken en niet verder gaan dan wat daarvoor geschikt en noodzakelijk is".3*

Waar het de rechterlijke toets in dit verband betreft, overweegt het Hof dat wanneer sprake is van een inmenging in fundamentele rechten, de omvang van de beoordelingsbevoegdheid van de wetgever van de Unie beperkt kan zijn. Het is dan juist van belang dat er strikt toezicht wordt uitgeoefend door de rechter.4

Waar het de noodzaak van de inbreuk op de grondrechten betreft, overweegt het Hof als volgt.

> *"51. Wat de noodzaak van de door richtlijn 2006/24 voorgeschreven bewaring van gegevens betreft, zij vastgesteld dat de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd.*
>
> *52. Wat het recht op eerbiediging van het privéleven betreft, zij opgemerkt dat de bescherming van dit fundamentele recht volgens vaste rechtspraak van het Hof hoe dan ook vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (arrest IPI, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).*
>
> *53. Dienaangaande zij eraan herinnerd dat de bescherming van persoonsgegevens, die uitdrukkelijk wordt voorgeschreven door artikel 8, lid 1, van het Handvest, van bijzonder belang is voor het in artikel 7 van dit Handvest verankerde recht op eerbiediging van het privéleven.*
>
> *54. De betrokken Unieregeling moet dus duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens […].*
>
> *55 De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens, zoals is bepaald in richtlijn 2006/24, automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd […]."*

Ook wordt overwogen:

---

3 Par. 46.
4 Par. 47 en 48.

"59. Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.

60. In de tweede plaats bevat richtlijn 2006/24 niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. Integendeel, richtlijn 2006/24 verwijst in artikel 1, lid 1, ervan enkel op algemene wijze naar ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

61. Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Artikel 4 van deze richtlijn, dat de toegang van deze autoriteiten tot de bewaarde gegevens regelt, bepaalt niet uitdrukkelijk dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen, maar bepaalt enkel dat elke lidstaat de procedure en de te vervullen voorwaarden vaststelt voor toegang tot de bewaarde gegevens overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid.

62. In het bijzonder bevat richtlijn 2006/24 geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel. Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Aan de lidstaten is evenmin enige specifieke verplichting opgelegd om dergelijke beperkingen vast te stellen.

Het brengt het Hof tot de slotsom dat richtlijn 2006/24 ongeldig is. Het belang van het arrest is groot. De overwegingen die zijn geciteerd, vormen uitgangspunten voor hierop volgende jurisprudentie, maar ook hoe tegen de onderhavige casus moet worden aangekeken.

Tele2, 21 december 2016, ECLI:EU:C:2016:970.

Het volgende arrest dat hier wordt besproken, betreft een procedure van Tele2 tegen de Zweedse staat. Die procedure vloeide voort uit het Digital Rights arrest. Nadat dit arrest was gewezen, stopte Tele2 met het verstrekken van de gegevens, die volgens richtlijn 2006/24 diende te worden bewaard, en volgens nationale wetgeving aan de toezichthoudende autoriteit voor post en communicatie (PTS) diende te worden verstrekt. PTS was het nationale orgaan dat de bewaarde gegevens op grond van art. 4 van richtlijn 2006/24 ontving.

Dit gebeurde op 9 april 2014, een dag na het wijzen van het Digital Rights arrest. Zes dagen later deed de Zweedse politie haar beklag bij PTS, omdat zij ineens geen data van Tele2 meer ontvingen. Er werd een commissie ingesteld om te onderzoeken of de Zweedse wetgeving omtrent de bewaarplicht van telecomaanbieders zich nog verhield tot het Unierecht, nu richtlijn 2006/24 ongeldig was verklaard. De betreffende commissie oordeelde dat dit zo was. Tele2 hield voet bij stuk en verstrekte geen gegevens meer. Een procedure bij de bestuursrechter ontstond, waarin de beoordeling van de Zweedse wetgeving in het licht van art. 15 lid 1 van richtlijn 2002/58, tegen de achtergrond van de artikelen 7, 8 en 52 van het Handvest centraal stond. De prejudiciële vragen die het Hof werden gesteld, hielden verband met de vraag hoe het algemeen en ongedifferentieerd bewaren van elektronische communicatiegegevens, zich verhoudt met de voornoemde Unierechtelijke bepalingen.

Het onderhavige arrest betrof overigens niet slechts de Zweedse procedure. In Groot-Brittannië liep ook een procedure waarin burgers zich op het standpunt stelde dat de Britse wetgeving over de bewaarplicht van de gegevens zich niet verhield met het Unierecht, sinds het ongeldig verklaren van richtlijn 2006/24. In die procedure concludeerde de Britse rechter in hoger beroep dat richtlijn 2002/58 niet van toepassing is op de betreffende wetgeving, onder verwijzing naar art. 1 lid 3 van de richtlijn. Daarin wordt benoemd dat de richtlijn niet van toepassing is op activiteiten die verband houden met “de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied”. Omdat in andere lidstaten reeds was geoordeeld dat de nationale wetgeving die voortvloeide uit richtlijn 2006/24 ongeldig was, sinds het Digital Rights arrest, erkende de Britse rechter wel dat er discussie kon bestaan over zijn visie, waardoor prejudiciële vragen werden gesteld.

Werkingssfeer.

Het Hof is in het onderhavige arrest daarom eerst gaan kijken naar de vraag of de nationale wetgeving die de verplichting aan elektronische communicatiediensten oplegt om gegevens te bewaren en aan nationale autoriteiten te verstrekken, valt binnen de werkingssfeer van het Unierecht. Is dat niet het geval, dan vindt er immers ook geen toets aan het Handvest plaats.

Het Hof is hierover heel duidelijk:

> *73. Gelet op de algemene opzet van richtlijn 2002/58, kan uit de in het voorgaande punt van het onderhavige arrest genoemde elementen echter niet worden afgeleid dat de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen van de werkingssfeer van deze richtlijn zijn uitgesloten, omdat daardoor aan deze bepaling elk nuttig effect zou worden ontnomen. Deze bepaling vooronderstelt immers noodzakelijkerwijze dat de aldaar bedoelde nationale maatregelen, zoals die betreffende de bewaring van gegevens ter bestrijding van criminaliteit, binnen de werkingssfeer van die richtlijn vallen, omdat in deze laatste uitdrukkelijk wordt bepaald dat de lidstaten die*

maatregelen slechts mogen treffen met inachtneming van de aldaar geformuleerde voorwaarden.

Het Hof benadrukt vervolgens dat het recht op bescherming van het vertrouwelijke karakter van de communicatie, als genoemd in art. 5, lid 1, van richtlijn 2002/58, geldt ten aanzien van eenieder. Voorts legt het uit dat de uitzonderingen op het uitgangspunt als genoemd in art. 15, lid 1, van richtlijn 2002/58, niet slechts geldt in verband met de opslag van de gegevens, maar ook voor het gebruik ervan.5

Verhouding art. 15, lid 1, richtlijn 2002/58, tot de artt. 7, 8, 11 en 52 Handvest.

Nu is geoordeeld dat de betreffende nationale wetgeving valt binnen de werkingssfeer van het Unierecht, speelt de vraag in hoeverre zich dat verhoudt tot de grondrechten die zijn genoemd in het Handvest. Opvallend in dit verband is dat de prejudiciële vragen die door de Zweedse rechter werden gesteld, de toets met de artikelen 7, 8 en 52 betrof. Het Hof betrekt er echter ook art. 11 van het Handvest bij, inhoudende de vrijheid van meningsuiting.

Vervolgens wijst het Hof in haar overwegingen over de interpretatie van art. 15 lid 1 van richtlijn 2002/58 eerst op de memorie van toelichting bij het voorstel voor de betreffende richtlijn, waaruit blijkt dat de Uniewetgever heeft *"willen zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronische communicatiediensten, ongeacht de gebruikte technologie."6*

In beginsel geldt een verbod op het zonder toestemming van de gebruikers opslaan van verkeersgegevens betreffende de elektronische communicatie. Hierop kan op grond van art. 15, lid 1, van de richtlijn een uitzondering worden gemaakt. Het Hof benadrukt voorts dat de principeverplichting tot waarborging van de vertrouwelijkheid strikt dient te worden uitgelegd. *"Een dergelijke bepaling kan dus niet rechtvaardigen dat de in artikel 5 van deze richtlijn bepaalde uitzondering op deze principeverplichting en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt, omdat laatstgenoemde bepaling in dat geval grotendeels haar inhoud zou verliezen."7*

De doelstellingen die in art. 15, lid 1, richtlijn 2002/58 zijn genoemd, zijn exhaustief, maar kunnen slechts een beperking van het in artikel 5 genoemde recht vormen, als dit in overeenstemming is met algemene beginselen en grondrechten die worden gewaarborgd door het Handvest.8 Het Hof slaat in dat verband, zoals reeds duidelijk is geworden, acht op de artikelen 7, 8 en 11 van het Handvest. Over de vrijheid van meningsuiting overweegt het Hof voorts dat dit "een van de wezenlijke grondslagen van een democratische en pluralistische samenleving [is], die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd".9

Na de bespreking van de grondrechten die aan de orde zijn, gaat het Hof in op art. 52 Handvest. Hieruit volgt dat een beperking van grondrechten bij moet worden gesteld en de wezenlijke inhoud van het grondrecht moet eerbiedigen. *"Met inachtneming van het evenredigheidsbeginsel kunnen*

5 Par. 78 en 79.
6 Par. 82.
7 Par. 89.
8 Par. 90 en 91.
9 Par. 93.

slechts beperkingen op de uitoefening van die rechten en vrijheden worden gesteld indien deze noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten vrijheden van anderen".10

Deze overweging wordt nader geconcretiseerd door de inhoud van art. 15, lid 1, richtlijn 2002/58. Aan het evenredigheidsbeginsel wordt voldaan, wanneer een maatregel *"in een democratische samenleving noodzakelijk, redelijk en proportioneel is".* Dit is het kader als geschetst door het EHRM, maar dat betekent niet dat de invulling daarvan zonder meer hetzelfde is. De waarborgen die het EHRM stelt, zijn immers minimumwaarborgen. De bescherming die het Handvest biedt, kan verder gaan.11

Het Hof verwijst naar overweging 11 van de richtlijn, waarin wordt gepreciseerd dat een maatregel als genoemd in art. 15 van de richtlijn, "strikt" evenredig moet zijn met het nagestreefde doel. *"Wat in het bijzonder de bewaring van gegevens betreft, eist artikel 15, lid 1, tweede zin, van deze richtlijn dat deze gegevens slechts "gedurende een beperkte periode" worden bewaard "om de redenen" die in artikel 15, lid 1, eerste zin, van die richtlijn worden genoemd".12*

Voornoemd kader, toegepast op de Zweedse wetgeving, leidt het Hof tot dezelfde overwegingen als gemaakt in het Digital Rights arrest. De nationale wetgeving komt namelijk grotendeels overeen met richtlijn 2006/24. Er wordt op gewezen dat bewaring van verkeersgegevens en van locatiegegevens alleen kan worden gerechtvaardigd als het de bestrijding van ernstige criminaliteit betreft.13 Daaraan is echter een grote maar verbonden:

> *"103. Daarbij komt dat de doeltreffendheid van de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een nationale regeling die voorzien in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens, noodzakelijk wordt geacht voor het voeren van deze strijd."*

De nationale regeling beoordeelt het Hof vervolgens als verder gaand dan strikt noodzakelijk en daarom niet gerechtvaardigd in een democratische samenleving.

Nationale regeling die het bepaalde in art. 15, lid 1, richtlijn 2002/58, regelt.

Het Hof gaat vervolgens in op de vraag hoe een nationale regeling die een beperking als bedoeld in art. 15, lid 1, van richtlijn 2002/58, regelt, eruit dient te zien.

Het hof benoemt nogmaals dat het bewaren van verkeers- en locatiegegevens preventief kan plaatsvinden ter bestrijding van zware criminaliteit. Dit dient echter tot het strikt noodzakelijke te worden beperkt, waar het de categorieën van te bewaren gegevens; betrokken communicatiemiddelen; de betrokken personen en de duur van de bewaring betreft.

10 Par. 94.
11 Art. 52 lid 3 Handvest.
12 Par. 95.
13 Par. 102.

De nationale regeling dient te voldoen aan het volgende:

1. Er bestaan duidelijke en nauwkeurige regels voor de draagwijdte en de toepassing van een dergelijke maatregel van bewaring van gegevens, alsmede minimumeisen, zodat de personen wier gegevens zijn bewaard, voldoende garanties hebben dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik;
    a. In het bijzonder dient te worden aangegeven in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen.
        i. Aldus wordt gewaarborgd dat een dergelijke maatregel tot het strikt noodzakelijke wordt beperkt.14
2. Waar de materiële voorwaarden voor de preventieve bewaring van gegevens per maatregel kan verschillen om het tot het strikt noodzakelijke te beperken, geldt dat de daadwerkelijke bewaring steeds moet voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel. In het bijzonder moeten dergelijke voorwaarden in de praktijk van dien aard blijken te zijn dat zij de omvang van de maatregel, en dus de kring van betrokken personen, daadwerkelijk afbakenen.
    a. De nationale regeling moet worden gebaseerd op objectieve elementen, waarmee kan worden gemikt op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid kan worden voorkomen.
        i. Een dergelijke afbakening kan aan de hand van een geografisch criterium worden verricht wanneer de bevoegde nationale autoriteiten op basis van objectieve elementen van mening zijn dat er in een meer geografische gebieden een hoog risico bestaat dat dergelijke handelingen worden voorbereid of gepleegd.15

In verband met de eis van strikte noodzakelijkheid, overweegt het Hof nog als volgt.

“119. Aangezien een algemene toegang tot alle bewaarde gegevens los van enig – zelfs ook maar indirect – verband met het nagestreefde doel niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, moet de betrokken nationale regeling dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationaliteiten autoriteiten toegang tot de gegevens van de abonnees of de geregistreerde gebruikers moet worden verleend. In dit verband kan in beginsel voor het doel van bestrijding van criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf (zie naar analogie EHRM, 4 december 2015, Zakharov tegen Rusland, CE:ECHR:2015:1204JUD004714306, § 260). In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot bestrijding van dergelijke activiteiten zouden kunnen leveren.

14 Par. 109.
15 Par. 110-111.

120. Om te waarborgen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze autoriteiten dat met name is ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten […].

Voorts wijst het Hof erop dat de betrokkenen zo spoedig mogelijk dienen te worden geïnformeerd over de maatregel, zodat de burger ook gebruik kan maken van het recht van beroep.16

Een en ander brengt het Hof tot de slotsom dat de Zweedse wetgeving in strijd was met richtlijn 2002/58.

Dit arrest is van belang voor de beoordeling van de vraag of maatregelen vallen binnen de werkingssfeer van het Unierecht, maar ook voor de beoordeling van de wetgeving die ten grondslag ligt aan de inzet van de maatregel, het gewicht van de betreffende grondrechten en de het evenredigheidsbeginsel.

Ministerio Fiscal, 2 oktober 2018, ECLI:EU:C:2018:788.

Voor de beoordeling van de vraag of maatregelen binnen de werkingssfeer van het Unierecht vallen, is ook dit arrest van belang. Voorts is dit arrest van belang voor het besef dat de invulling van het evenredigheidsbeginsel, niet statisch is.

Dit arrest betreft een Spaanse strafzaak, waarin een diefstal met geweld werd onderzocht. Hierbij was een mobiele telefoon gestolen. Elf dagen na het delict deed de gerechtelijke politie een verzoek aan de Spaanse onderzoeksrechter om verschillende aanbieders van elektronische communicatiediensten te gelasten de telefoonnummers door te geven die in die elf dagen waren gekoppeld aan het IMEI-nummer van de gestolen telefoon, alsmede de persoonsgegevens van de gebruikers van die telefoonnummers. Dit verzoek werd door de rechter-commissaris afgewezen, omdat het geen ernstig feit betrof. Volgens de Spaanse wet (destijds), kon onder “ernstige delicten” een delict worden verstaan waarvoor een gevangenisstraf van vijf jaar of meer kon worden gegeven. Daarvan was geen sprake. Het leidde uiteindelijk tot het stellen van prejudiciële vragen, waarbij ook de vraag aan de orde was of dergelijke onderzoeken vielen binnen de reikwijdte van het Unierecht. Daarbij werd wederom gewezen op art.1 lid 3 van richtlijn 2002/58.

Het Hof heeft hier vervolgens uitgelegd wat dient te worden verstaan onder “activiteiten van de staat”, als genoemd in dat artikel. *“De in die bepaling als voorbeeld genoemde activiteiten zijn in alle gevallen specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien.”17* Ook hier wijst het Hof er weer op dat wanneer de interpretatie zou worden gevolgd, dat art. 1 lid 3 van de richtlijn in de weg staat aan de conclusie dat de maatregel binnen de werkingssfeer van de richtlijn, dat elk nuttig effect aan art. 15, lid 1, van de richtlijn zou worden ontnomen.

In verband met het evenredigheidsbeginsel overweegt het Hof dat art. 15, lid 1, niet slechts beperkingen van de genoemde grondrechten toestaat bij ernstige criminaliteit, maar reeds ter

16 Par. 121.
17 Par. 32.

zake het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.18 Het is de ernst van de inmenging in die grondrechten, dat bepaalt wat de ernst van de criminaliteit is die ermee wordt getracht te bestrijden.

In de onderhavige casus achtte het Hof de inbreuk op de betreffende grondrechten beperkt, waardoor het doel in verhouding stond tot het middel.

Privacy international, 6 oktober 2020, ECLI:EU:C:2020:790.

Op 6 oktober 2020 heeft het Hof een tweetal arresten gewezen in verband met de onderhavige materie. Het eerste arrest betreft de beantwoording van prejudiciële vragen in een Britse zaak. De NGO Privacy International had een procedure aangespannen tegen de handelswijze van de staat, die bestond uit het vergaren en gebruiken van bulk communicatiedata door de veiligheidsdiensten.

De bulkdata die werden vergaard bestonden uit biografische gegevens of reisbewegingen, financiële of commerciële informatie of communicatiedata, waaronder mogelijke geheimhoudingsinformatie. Het gebruik van de data bestond uit een analyse door middel van “cross-checking” (data vergelijken met data die vanwege andere onderzoeken zijn verkregen) en geautomatiseerde zoeksystemen. Bovendien kon de data worden gedeeld met andere personen, autoriteiten of buitenlandse partners. Het vergaren en gebruiken van de data, gebeurde op grond van nationale wetgeving. De prejudiciële vragen die werden gesteld betroffen wederom de vraag of de maatregelen vielen binnen de werkingssfeer van het Unierecht, als ook hoe de maatregelen zich verhielden tot richtlijn 2002/58.

Omdat het hier niet de opsporing van ernstige strafbare feiten betrof, maar de nationale veiligheid, stelde de Britse staat zich op het standpunt dat de maatregelen niet vielen binnen de werkingssfeer van het Unierecht. Daarbij werd gewezen op art. 4 lid 2 VEU, waaruit volgt dat de nationale veiligheid een aangelegenheid is van de lidstaten zelf. De overwegingen van het Hof over dit standpunt wijkt niet af van de overwegingen in verband met art. 1 lid 3, richtlijn 2002/58, zoals eerder besproken. De maatregelen, voor zover deze betreffen het verplichten van elektronische communicatiediensten tot het bewaren en verstrekken van gegevens, vallen aldus binnen de werkingssfeer van het Unierecht, meer specifiek richtlijn 2002/58.

Het Hof staat vervolgens stil bij de inhoud van de maatregelen, de informatie die wordt verzameld, het feit dat dit algemeen en ongedifferentieerd gebeurt en dat de informatie door de veiligheidsdienst wordt opgeslagen en voor hen beschikbaar blijft. Het Hof overweegt, zoals zij ook deed in Digital Rights en Tele2 dat het uitgangspunt is dat de lidstaten de vertrouwelijkheid van elektronische communicatie waarborgen en hier ook maatregelen voor treffen. Weliswaar biedt art. 15 een uitzondering op die verplichting, maar dat kan niet betekenen dat de uitzondering de regel wordt.

Het Hof benoemt wederom dat met het treffen van maatregelen als de onderhavige, art. 7 en 8 van het Handvest in het geding komen, alsmede de vrijheid van meningsuiting als genoemd in art. 11 van het Handvest. Wederom benadrukt het Hof het belang van die grondrechten. Vervolgens overweegt hij dat de rechten niet absoluut zijn, maar de beperking kan plaatsvinden gelet op het bepaalde in art. 52 lid 1 Handvest. Over de eis dat de beperking is voorzien bij wet, overweegt het hof dat die wet ook de reikwijdte van de beperking moet vastleggen.19 De maatregelen dienen tot het strikt noodzakelijke worden beperkt, hetgeen dient te worden

18 Par. 56.
19 Par. 65.

gewaarborgd door de betreffende wet. Het bestaan van waarborgen wordt des te klemmend, wanneer de maatregel het automatisch verzamelen van persoonlijke data betreft, meer in het bijzonder als een aanzienlijk risico bestaat op onrechtmatige toegang tot die data. Dat geldt te meer wanneer de persoonlijke informatie, gevoelige informatie betreft.20

Dan staat het Hof stil bij het feit dat het algemeen en ongedifferentieerd verzamelen van verkeers- en locatiegegevens betekent dat de uitzondering op de bescherming van de grondrechten, de regel is geworden. Erkend wordt dat het belang van nationale veiligheid van aanzienlijk zwaarder gewicht is dan andere doelstellingen die in art. 15 lid 1 richtlijn 2002/58 worden genoemd, maar dat dit niet wegneemt dat voorwaarden als hiervoor genoemd, zijn vereist. Nu dat niet het geval is, kan niet worden geoordeeld dat de maatregelen zijn beperkt tot hetgeen strikt noodzakelijk is. Het Hof concludeert dan ook dat de wetgeving die het mogelijk maakt om elektronische communicatiediensten te verplichten om algemeen en ongedifferentieerd verkeers- en locatiegegevens op te slaan en te verstrekken aan de veiligheidsdiensten, in strijd is met art. 15, lid 1, van richtlijn 2002/58, tegen de achtergrond van art. 4 lid 2 VEU en art. 7, 8, 11 en 52 lid 1 van het Handvest.

La Quadrature du Net, 6 oktober 2020, ECLI:EU:C:2020:791.

Dit betreft het tweede arrest dat het Hof op 6 oktober 2020 heeft gewezen. In dit arrest wordt ingegaan op vragen die in twee verschillende Franse procedures werden gesteld, alsmede op vragen die in een Belgische procedure werden gesteld. Dit arrest is in het bijzonder relevant voor de beoordeling van het gebruik van Encrochatdata.

Waar gaat het over?

In de eerste Franse procedure, procedeert de elektronische communicatiedienst La Quadrature du Net, tegen de Franse staat, vanwege wetgeving, die het mogelijk maakt de elektronische communicatiedienst te verplichten om in hun netwerk een automatische dataverwerker te installeren, die is ontwikkeld om verbanden te vinden met een terroristische dreiging. Weliswaar werd hiermee alle communicatiedata verwerkt, maar slechts voor een beperkte tijd. De bedoeling is om slechts de data betreffende dergelijke serieuze feiten te verzamelen. Bovendien werden er maatregelen getroffen die de elektronische communicatiedienst niet verplichte om gegevens te bewaren. De Franse autoriteiten bewaarden de data zelf.

De tweede Franse procedure was ook aangespannen door La Quadrature du Net, en betreft het algemeen en ongedifferentieerd bewaren van inhoudelijke communicatie. Daar onderscheid deze procedure zich van eerder genoemde procedures, die gaan over het verwerken van verkeers- en locatiedata. Waar deze zaak zich ook onderscheid van andere procedures, is dat het hier niet de data van publiekelijk toegankelijke elektronische communicatiediensten betreft van elektronische communicatienetwerken in de EU. Het gaat hier over online communicatiediensten.

De Belgische zaak betrof ook de verplichting aan aanbieders van telefonische diensten, waaronder via internet; van internettoegang; van e-mail via internet of van openbare elektronische communicatienetwerken om data te bewaren, ten behoeve van het onderzoeken, opsporen en vervolgen van zaken betreffende het seksueel misbruik van kinderen.

De vragen die in deze procedure werden gesteld, betroffen niet slechts de werkingssfeer en de verhouding tussen de maatregelen en richtlijn 2002/58, tegen de achtergrond van het Handvest.

20 Par. 67 en 68.

Ook kwam richtlijn 2000/31 aan bod, welke “bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt” betreft. De vraag die hierover werd gesteld, is of het de staat mogelijk maakt nationale wetgeving te creëren, waardoor personen, wiens activiteiten bestaan uit het aanbieden van toegang tot online publieke communicatiediensten, of natuurlijke of rechtspersonen die, ook al ligt daaraan geen vergoeding ten grondslag, om het publiek te voorzien van online communicatiediensten, signalen, schrijven, afbeeldingen, geluiden of berichten van welke aard ook, welke door de gebruiker van de dienst worden geleverd, opslaan, kunnen worden verplicht om de data te bewaren die het mogelijk maken iemand te identificeren die heeft bijgedragen aan de creatie van een bepaalde inhoud, of deel daarvan, van de diensten die worden geleverd, zodat een judiciële autoriteit, waar passend, de communicatie in die data kan opeisen om te onderzoeken of wordt voldaan aan civiele en strafrechtelijke aansprakelijkheden.

Ook richtlijn 2016/680, speelt in dit arrest een rol, hetgeen de bescherming van natuurlijke personen betreft, in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten, met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Tot slot, passeert ook de AVG, verordening 2016/679, de revue.

Werkingssfeer.

Het Hof heeft belangrijke overwegingen gewijd aan de werkingssfeer van richtlijn 2002/58. De Franse autoriteiten hadden namelijk geen verplichting gecreëerd, waardoor elektronische communicatiediensten data moesten bewaren, maar een verplichting om autoriteiten toegang tot de data te verlenen. Ook dit viel echter binnen de werkingssfeer van richtlijn 2002/58, omdat de wetgevende maatregel noodzakelijkerwijs een verwerkingsverplichting op de aanbieders legde.21

Vervolgens wordt benoemd dat richtlijn 2002/58 een lex specialis is van de AVG. De interpretatie van art. 1, lid 3, van de richtlijn, geldt ook voor de interpretatie van art. 2, lid 2, ahf en onder d van de AVG. De interpretatie van art. 15 van de richtlijn, is hetzelfde als de interpretatie van art. 23 van de AVG.22

Als het gaat om directe maatregelen die de staat inzet om een inbreuk te maken op het recht op vertrouwelijkheid van elektronische communicatie, zonder verplichtingen op te leggen aan elektronische communicatiediensten, dan valt dit niet binnen de werkingssfeer van richtlijn 2002/58. Dit vindt plaats op basis van nationale regelgeving, wat dan wel valt binnen de werkingssfeer van richtlijn 2016/680 en dus het Unierecht. Dit betekent voorts dat de maatregelen dienen te voldoen aan de nationale grondwet en de vereisten van het EVRM.23

Algemene en ongedifferentieerde verzameling van gegevens in het licht van de doelstelling.

Waar het Hof in dit arrest voorts meer aandacht aan besteedt, dan in eerder genoemde arresten, is de verhouding tussen de plicht van een lidstaat, om bescherming te bieden aan het recht op family life en privacy, waaronder het recht op de bescherming van het huis en de communicatie

21 Par. 96.
22 Par. 102.
23 Par. 103.

van de individu enerzijds en de plicht van een lidstaat om de fysieke en psychische integriteit van individuen te beschermen en te voorkomen dat er martelingen of inhumane of vernederende behandeling plaatsvinden. Er wordt in dit verband allereerst acht geslagen op de rechtspraak van het EHRM, waaruit volgt dat er formele voorzieningen en praktische maatregelen moeten kunnen worden getroffen, waardoor er effectief kan worden opgetreden tegen misdrijven, door effectieve opsporing en vervolging. Die maatregelen moeten andere vrijheden en rechten echter wel respecteren. Een juridisch kader dient te worden gecreëerd, waardoor een balans kan worden verkregen.

Vervolgens wijst het Hof weer op art. 15, lid 1, Handvest, waaruit volgt dat maatregelen noodzakelijk, redelijk en proportioneel dienen te zijn, waarbij, gelet op paragraaf 11 van de preambule, dient te worden benadrukt dat de maatregel strikt noodzakelijk dient te zijn, in het licht van het beoogde doel.

De vraag of de beperking van grondrechten als genoemd in richtlijn 2002/58 is gerechtvaardigd, hangt af van de omvang van de beperking en wat het gewicht is van het publieke belang dat wordt getracht te waarborgen. Daarbij zijn verschillende publieke belangen te onderscheiden, waar het Hof op ingaat:

1. **Nationale veiligheid**. In dit verband gaat het over het voorkomen en bestraffen van activiteiten die fundamentele constitutionele, politieke, economische of sociale structuren van een staat ernstig kunnen destabiliseren, waarbij het in het bijzonder gaat om een directe dreiging van de maatschappij, de bevolking of de staat zelf, zoals een terroristische daad. Slechts in die gevallen zou er een maatregel kunnen worden getroffen die de algemene en ongedifferentieerde opslag van data inhoudt. Daarvoor is dan wel van belang dat er daadwerkelijke controle op het gebruik van een dergelijke maatregel plaatsvindt door een rechtbank, of ander onafhankelijk administratief orgaan. De controle dient te zien op de vraag of er sprake is van een situatie als voornoemd, maar ook op de voorwaarden en waarborgen die daarbij worden gesteld.24

2. **Bestrijding criminaliteit en beschermen publieke veiligheid.** Wanneer dit het doel is, dan rechtvaardigt slechts de bestrijding van ernstige criminaliteit, een ernstige inbreuk op de rechten als genoemd in art. 7 en 8 van het Handvest. Deze doelstelling, zelfs als het de bestrijding van ernstige criminaliteit betreft, rechtvaardigt nooit wetgeving die voorziet in de algemene en ongedifferentieerde opslag van verkeers- en locatiegegevens. Zelfs wanneer wordt gekeken naar de positieve verplichting die op staten rust om inbreuken op andere grondrechten te bestrijden, is handelen dat even ernstig is als voornoemde wetgeving, niet gerechtvaardigd. Benadrukt wordt dat het voornoemde dus niet geldt in een situatie waarin maatregelen worden genomen tegen een reeds bekende verdachte en waarbij objectief bewijs ten grondslag ligt aan de aangenomen dreigen van de publieke of nationale veiligheid.

   Ook wordt besproken dat de grenzen van een maatregel die voorziet in de bewaring van verkeers- en locatiedata, kunnen worden bepaald aan de hand van een geografisch criterium, waarbij de competente autoriteiten op basis van objectieve en non-discriminatoire factoren, waaruit volgt dat er in die gebieden een situatie bestaat, waaruit een hoog risico volgt op de voorbereiding of het plegen van ernstige strafbare feiten. Het kan dan gaan over gebieden waarin veel ernstige criminaliteit plaatsvindt, of die hiervoor

24 Par. 139.

extra gevoelig zijn, zoals infrastructurele gebieden waarin zeer hoge volumes aan bezoekers komen, of strategische plaatsen, zoals vliegvelden, stations of tolpoorten. Wanneer het over maatregelen in dit soort gebieden gaat, dient nog steeds het proportionaliteitsbeginsel in acht te worden genomen. Bewaring van gegevens mag niet langer duren dan wat strikt noodzakelijk is in het licht van het nagestreefde doel en de omstandigheden waaronder de inbreuk is gerechtvaardigd.25

In dit verband worden nog belangrijke overwegingen gewijd aan een situatie waarin de wettelijke bewaartermijn van gegevens voor elektronische communicatiediensten eindigt, maar het toch van belang kan zijn om die gegevens te bewaren om ernstige strafbare feiten of handelingen die de nationale veiligheid schaden, aan het daglicht te brengen. Dat kan aan de orde zijn bij strafbare feiten die reeds zijn vastgesteld, of bij een redelijk vermoeden van dergelijke strafbare feiten, op basis van objectief onderzoek van alle relevante omstandigheden. Er is voor dergelijke situaties wetgeving mogelijk op basis waarvan, onder effectieve rechterlijke toetsing, een besluit mogelijk is waarin elektronische communicatiediensten worden verplicht tot het versneld bewaren van verkeers- en locatiegegevens voor een bepaalde periode. Uit de wetgeving moet dan de doelstelling blijken die dit rechtvaardigt. Het mag slechts gaan over verkeers- en locatiegegevens die licht kunnen schijnen op ernstige strafbare feiten of handelingen die de nationale veiligheid in gevaar brengen en de bewaringstermijn dient te worden beperkt tot het strikt noodzakelijke.

Het hoeft in dit kader niet te gaan om gegevens van verdachte. Een dergelijke maatregel kan, binnen de grenzen van het strikt noodzakelijke, worden uitgebreid tot die verkeers- en locatiegegevens met betrekking tot andere personen dan degenen die ervan worden verdacht een ernstig strafbaar feit te hebben gepland of gepleegd, op voorwaarde dat die gegevens, op basis van objectieve en niet-discriminerende factoren, licht werpen op een dergelijk strafbaar feit. Voorbeelden zijn gegevens over het slachtoffer, zijn of haar sociale of professionele kring, of zelfs specifieke geografische gebieden, zoals de plaats waar het strafbare feit is gepleegd. Een en ander kan uiteraard slechts dan, als het in overeenstemming is met de beginselen die in de jurisprudentie van het Hof zijn genoemd.

Real-time analyse van data.

Volgens het Hof valt ook de real-time geautomatiseerde analyse onder richtlijn 2002/58. Het staat niet in de weg aan het creëren van nationale regels hieromtrent, zolang de toepassing van de analyse maar wordt beperkt tot de situaties waarin de nationale veiligheid ernstig wordt bedreigd, waarvan is aangetoond dat deze reëel en aanwezig of voorzienbaar is, waarin een dergelijke analyse kan worden onderworpen aan een doeltreffende beoordeling, hetzij door een rechtbank of door een onafhankelijk bestuursorgaan waarvan de beslissing bindend is, met als doel na te gaan of een situatie bestaat die die maatregel rechtvaardigt en of voorwaarden en waarborgen die moeten worden gesteld, worden nageleefd. Als het gaat om real-time verzameling van verkeers- en locatiegegevens, dan geldt dat dit dient te worden beperkt tot personen van wie er een gegronde reden is om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, welk vermoeden is onderworpen aan een voorafgaand onderzoek door een rechtbank om ervoor te zorgen dat een dergelijke real-time verzameling alleen wordt toegestaan binnen de grenzen van wat strikt noodzakelijk is.

25 Par. 150-151.

Openbare onlinecommunicatiediensten en aanbieders van hostingdiensten.

De volgende vraag die het Hof behandelt, betreft de beoordeling van methodieken die niet vallen onder richtlijn 2002/58. Hierboven betrof het telkens maatregelen die vielen binnen de werkingssfeer van richtlijn 2002/58. Om in die werkingssfeer te vallen, is het van belang dat er bewaar- cq. deelverplichtingen worden opgelegd aan elektronische communicatiediensten. Maar als een lidstaat de informatie op een andere manier vergaart, valt dat dus niet onder richtlijn 2002/58. In dit geval betrof het nationale wetgeving die aanbieders van toegang tot openbare onlinecommunicatiediensten en aanbieders van hostingdiensten verplicht om algemeen en ongedifferentieerd onder andere persoonsgegevens met betrekking tot die diensten te bewaren. De verwijzende rechter oordeelde dat dit niet viel binnen de werkingssfeer van richtlijn 2002/58, maar wel binnen de werkingssfeer van richtlijn 2000/31. In die richtlijn staat echter geen verbod op het bewaren van gegevens, waarvan slechts bij uitzondering zou kunnen worden afgeweken. Dat neemt echter niet weg dat, omdat het valt binnen de werkingssfeer van het Unierecht, er een inbreuk wordt gemaakt op de grondrechten als bedoeld in art. 6, 7, 8 en 11 van het Handvest. De verwijzende rechter vroeg zich af hoe dit dan dient te worden beoordeelt.

Het Hof overwoog dat de visie van de verwijzende rechter, inhoudende dat de betreffende wetgeving niet viel binnen de werkingssfeer van richtlijn 2002/58, onjuist was. In richtlijn 2000/31 is bepaald dat die richtlijn niet van toepassing is op vraagstukken betreffende de diensten van de informatiemaatschappij die onder richtlijn 95/46 en 97/66 vallen. Uit de preambule van richtlijn 2000/31 blijkt dat de bescherming van de vertrouwelijkheid van communicatie en van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in het kader van diensten van de informatiemaatschappij, alleen wordt geregeld door richtlijnen 95/46 en 97/66. Richtlijn 2002/58 is de vervanger van richtlijn 97/66. De AVG (verordening 2016/679) is de vervanger van richtlijn 95/46. Vragen met betrekking tot de bescherming van de vertrouwelijkheid van communicatie en persoonsgegevens moeten dus worden beoordeeld op basis van richtlijn 2002/58 en verordening 2016/679.26

Richtlijn 2002/58 is namelijk een lex specialis van de AVG. Valt een maatregel niet onder richtlijn 2002/58, dan valt het onder de AVG. In de uitspraken die eerder in dit stuk aan bod kwamen, is uitgebreid uiteengezet hoe de beperking van het recht op de vertrouwelijkheid van communicatie, aan de hand van art. 15 van richtlijn 2002/58 dient te worden beoordeeld. Wanneer de maatregel echter niet valt binnen de werkingssfeer van richtlijn 2002/58, en dus wel binnen de werkingssfeer van de AVG, dan wordt het juridisch kader voor de beoordeling van de rechtmatigheid van de beperking van het recht op die vertrouwelijkheid, mede gevormd door art. 23 van de AVG, in het licht van de terzake doende bepalingen van het Handvest.

Terugkomend op de vraag of de aanbieders van toegang tot openbare onlinecommunicatiediensten en aanbieders van hostingdiensten elektronische communicatiediensten betreffen, waardoor de betreffende wetgeving zou vallen binnen de werkingssfeer van richtlijn 2002/58, verwijst het Hof naar richtlijn 2002/21. In deze richtlijn is de definitie van een elektronische communicatiedienst gegeven:

> *"*een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische-

26 Par. 199.

communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd […]".

Gelet op de definitie en hetgeen is overwogen in het Skype Communications-arrest27, oordeelt het Hof dat internettoegangsdiensten en webgebaseerde e-maildiensten ook elektronische communicatiediensten betreffen.28

Als het gaat over de interpretatie van art. 23 AVG, overweegt het Hof dat het doel van de AVG onder andere is dat er een hoog niveau van bescherming van natuurlijke personen binnen de EU wordt gewaarborgd, door een consistente en homogene toepassing van regels te verzekeren, die de fundamentele rechten en vrijheden van dergelijke natuurlijke personen beschermen, meer specifiek met betrekking tot de verwerking van persoonsgegevens in de hele Europese Unie. Daarom dient iedere verwerking van persoonsgegevens plaats te vinden in overeenstemming met de hoofdstukken II en III van de AVG, behoudens de afwijkingen die conform art. 23 zijn toegestaan.

Dit artikel kan niet aldus worden uitgelegd dat het lidstaten de bevoegdheid verleent om de eerbiediging van het privéleven te ondermijnen, zonder rekening te houden met de waarborgen uit het Handvest. Het kan voorts alleen gebeuren in overeenstemming met het evenredigheidsvereiste, zoals dat ook geldt bij art. 15 van richtlijn 2002/58. Afwijkingen en beperkingen van de bescherming van persoonsgegevens kan slechts aan de orde zijn als dat strikt noodzakelijk is. De overwegingen in verband met art. 15 richtlijn 2002/58, gelden mutatis mutandis voor art. 23 van de AVG.29

Wat als de wetgeving in strijd is met Unierecht?

De Belgische verwijzend rechter stelde vragen over de rechtmatigheid van wetgeving over het verzamelen en verwerken van data, met het oog op de opsporing en vervolging van kindermisbruik. Daarbij wilde de verwijzend rechter in wezen vernemen of een nationale bepaling die in strijd is met het Unierecht, alsnog voor enige tijd kan worden gebruikt. Ook was de vraag wat er in een strafproces dient te gebeuren met de informatie die is verzameld middels een methodiek, voordat de nationale bepaling die daarvoor de grondslag bood, in strijd met het Unierecht werd bevonden. Met name die laatste vraag is hier interessant.

In verband met de eerste vraag overweegt het Hof dat slechts hij, in uitzonderlijke gevallen, op basis van dwingende overwegingen van rechtszekerheid kan toestaan dat een Unierechtelijke regel tijdelijk wordt opgeschort, waardoor daarmee strijdig nationaal recht kan worden toegepast. Die toestemming kan slechts worden gegeven in het feitelijke arrest waarin over de uitlegging wordt beslist. Daarbij wordt overwogen dat het primaat en de uniforme toepassing van het Unierecht zou worden ondermijnd indien de nationale rechters de bevoegdheid zouden hebben om bepalingen van nationaal recht voorrang te geven op het Unierecht dat door de nationale bepaling wordt geschonden.30

Wat betreft de vraag over wat in een strafprocedure kan worden gedaan met de informatie die is verkregen middels een methodiek die in strijd met het Unierecht is gebleken, wijst het Hof op de verantwoordelijkheid van lidstaten. Op basis van het gelijkwaardigheidsbeginsel, is het aan de nationale rechter die strafprocedures behandelt, om te bepalen wat er dient te gebeuren met deze

27 HvJ EU 5 juni 2019, *Skype Communications,* ECLI:EU:C:2019:460
28 Par 205.
29 Par. 207-211.
30 Par. 217.

informatie. Daarbij is opgemerkt dat wanneer het gebruik in strijd is met het recht op een eerlijk proces, het niet kan worden gebruikt. Als voorbeeld wordt benoemd dat de verdachte niet in staat is om effectief commentaar te leveren op die informatie en dat bewijsmateriaal en zij betrekking hebben op een gebied waarvan de rechters geen kennis hebben en waarschijnlijk een overheersende invloed zullen hebben op de feitelijke vaststellingen.

Valt het gebruik van Encrochatdata binnen de werkingssfeer van het Unierecht?

Vergaren versus bewaren en gebruiken.

Uit de stukken die door het OM zijn verstrekt over de verkrijging van de Encrochatdata, blijkt dat het OM een heel duidelijke tweedeling heeft willen maken. Beschreven wordt dat het onderscheppen van de Encrochatdata een Franse aangelegenheid was, waaraan de Nederlandse autoriteiten geen deel hebben genomen. Het leidt hen tot de conclusie dat voor zover het de rechtmatigheid van die verkrijging betreft, dat vanwege het vertrouwensbeginsel hier geen onderwerp van onderzoek betreft. In dit stuk wordt niet nader ingegaan op de rechtmatigheid van de verkrijging van de Encrochatdata in Frankrijk. Waar hier wel nader op in wordt gegaan, is het bewaren en gebruiken van die data in Nederland.

In de visie van de verdediging staat de mogelijke rechtmatigheid van de verkrijging namelijk los van de rechtmatigheid van het bewaren en gebruiken van die data, zoals dit in Nederland gebeurt. Het is het bewaren en gebruiken van de data, waarvan de verdediging stelt dat het in strijd is met het Unierecht. Waar het gaat over de vraag of het gebruik van de Encrochatdata binnen de werkingssfeer van het Unierecht valt, onderzoekt de verdediging dus niet de vraag of het verkrijgen van de data in Frankrijk binnen die werkingssfeer valt.

Overwegingen werkingssfeer nationale rechter.

In de nationale rechtspraak zijn inmiddels wat overwegingen gewijd aan de vraag of het gebruik van de Encrochatdata valt binnen de werkingssfeer van het Unierecht. De conclusies zijn de navolgende:

Rechtbank Amsterdam, 18 december 2020, ECLI:NL:RBAMS:2020:6443.

> *"Gelet op het voorgaande is de rechtbank op dit moment van oordeel dat voor zover de verdediging ter onderbouwing van haar onderzoekswensen heeft verwezen naar de hiervoor aangehaalde EU-richtlijn en de arresten van het HvJ-EU van 6 oktober 2020, dat onvoldoende is voor toewijzing van de verzoeken. In de EU-richtlijn 2002/58 is immers in artikel 1 lid 3 bepaald dat deze richtlijn niet van toepassing is op activiteiten van de Staat op strafrechtelijk gebied en in de genoemde arresten gaat het om een door nationale overheden opgestelde nationale regeling en niet, zoals in de onderhavige zaak, om een door de Franse autoriteiten uitgevoerd strafrechtelijk onderzoek."*

Rechtbank Rotterdam, 22 december 2020, ECLI:NL:RBROT:2020:11947.

> *"Uit het bepaalde in artikel 15, lid 1 van Europese Richtlijn 2002/58 volgt dat, behalve voor de nationale veiligheid, ook andere uitzonderingen op artikel 5, lid 1 van de Richtlijn kunnen worden gemaakt, bijvoorbeeld voor de wetshandhaving op strafrechtelijk gebied. De richtlijn doet met name geen afbreuk aan de mogelijkheid van lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren wanneer dat voor die wetshandhaving nodig is. De lidstaten dienen daarbij uiteraard wel het EVRM in acht te nemen (vgl. pag. 3 vertaling arrest HvJ EU).*
>
> *Ook in artikel 1, lid 3 van de Europese Richtlijn 2002/58 is bepaald dat deze niet van toepassing is op activiteiten van een lidstaat op strafrechtelijk gebied.*

> *In dit geval gaat het om de verzameling gegevens van elektronische communicatie ten behoeve van een strafrechtelijk onderzoek, wat -zoals gezegd- is uitgesloten van de werkingssfeer van de Europese Richtlijn 2002/58. Anders dan door de verdediging is betoogd, is het niet zo dat in de arresten van het HvJ EU is bepaald dat gegevensverzameling van elektronische communicatie alleen maar mag als sprake is van een ernstige bedreiging van de nationale veiligheid. Dit berust op een verkeerde lezing van de arresten."*

In beide zaken heeft de rechtbank voorlopig geoordeeld over het standpunt dat het gebruik van de Encrochatdata valt binnen de werkingssfeer van richtlijn 2002/58. In beide zaken, lag aan het oordeel dat dit niet valt binnen de werkingssfeer van die richtlijn, de interpretatie van art. 1 lid 3 van die richtlijn ten grondslag. Uit de bespreking van de jurisprudentie van het Hof, zoals hierboven is gedaan, blijkt in ieder geval de onjuistheid van dat oordeel. Het meest expliciet blijkt dit uit het arrest Ministerio Fiscal, van 2 oktober 2018, waarin de Spaanse staat ditzelfde standpunt ook innam.

Wanneer het gaat over de activiteiten van de staat, als benoemd in dat artikel, dan gaat het echter *"in alle gevallen* over *specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien".* Dat het gebruik van Encrochatdata wel degelijk iets van doen heeft met de gebieden waarop particulieren activiteiten ontplooien, moge duidelijk zijn. Met het gebruik wordt juist getracht daarin inzicht te verkrijgen. Aldus sluit artikel 1 lid 3 van richtlijn 2002/58 het gebruik van de Encrochatdata niet uit van de werkingssfeer van het Unierecht.

Het is hierbij niet verkeerd om stil te staan bij wat het Hof in de Tele2-zaak over ditzelfde standpunt overwoog:

> *73. Gelet op de algemene opzet van richtlijn 2002/58, kan uit de in het voorgaande punt van het onderhavige arrest genoemde elementen echter niet worden afgeleid dat de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen van de werkingssfeer van deze richtlijn zijn uitgesloten, omdat daardoor aan deze bepaling elk nuttig effect zou worden ontnomen. Deze bepaling vooronderstelt immers noodzakelijkerwijze dat de aldaar bedoelde nationale maatregelen, zoals die betreffende de bewaring van gegevens ter bestrijding van criminaliteit, binnen de werkingssfeer van die richtlijn vallen, omdat in deze laatste uitdrukkelijk wordt bepaald dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de aldaar geformuleerde voorwaarden.*

De interpretatie die zowel de rechtbank Rotterdam als de rechtbank Amsterdam geven van art. 1 lid 3 van Richtlijn 2002/58 geven is dus niet slechts onjuist. Het druist in tegen de kern van de bedoeling van de richtlijn.

Werkingssfeer richtlijn 2002/58.

Art. 1 lid 3 van Richtlijn 2002/58 maakt dus geenszins dat het bewaren en gebruiken van de Encrochatdata niet valt binnen de werkingssfeer van die richtlijn. De vraag die beantwoord dient te worden is niet of er redenen zijn waarom deze handelingen niet binnen de werkingssfeer van die richtlijn valt, maar of er redenen zijn waarom dit wel zo is.

Ik sta in dit verband ook stil bij dd bij argumentatie van het OM in de zaak 26Douglasville, wat mede ten grondslag ligt aan het standpunt dat de handelingen niet binnen de werkingssfeer van de richtlijn vallen. Blijkens de beslissing van de rechtbank, houdt die argumentatie in dat het in die zaak niet gaat *"om de vraag of een Staat wetgeving mag maken die telecomproviders verplicht*

de communicatiegegevens van al haar klanten/gebruikers te bewaren ten behoeve van het werk van inlichtingen- en veiligheidsdiensten. Het gaat om een strafzaak waarin een rechter op basis van een verdenking van een ernstig misdrijf, gemotiveerd, met toepassing van de eigen regels van het Wetboek van Strafvordering, een machtiging heeft verleend om bij de verdachte (alle) voor de beoordeling van die verdenking relevante data in beslag te nemen".31

In de visie van de verdediging kan uit deze overweging niet worden afgeleid dat het onderhavige bewaren en gebruiken niet binnen de werkingssfeer van het Unierecht valt. Nationale wetgeving moet immers conform het Unierecht worden geïnterpreteerd, wanneer het binnen de werkingssfeer van het Unierecht valt. Dat nationale regelgeving wordt toegepast, zegt dus niets over de vraag of met toepassing van die regelgeving, binnen de werkingssfeer van het Unierecht wordt geacteerd.

Waar het OM voorts stelt, dat het in de zaak waaraan wordt gerefereerd (de arresten van het HvJ EU van 6 oktober 2020), slechts gaat om het bewaren van gegevens ten behoeve van de inlichtingen- en veiligheidsdiensten, moge inmiddels duidelijk zijn dat dit niet zo is. Het gaat juist ook over het verschil in conclusie over de rechtmatigheid in het licht van het evenredigheidsbeginsel, wanneer er sprake is van verschillende doelstellingen, waarbij ook uitdrukkelijk en veel aandacht wordt besteed aan de opsporing van strafbare feiten.

Encrochat een elektronische communicatiedienst?

Voorts kan uit de argumentatie worden afgeleid dat het OM het standpunt inneemt dat het bij richtlijn 2002/58 gaat over telecomproviders. Dat is, zoals ook blijkt uit het La Quadrature du Net-arrest, een te beperkte lezing van het begrip elektronische communicatiedienst. Het dient te gaan over een dienst die, gewoonlijk tegen vergoeding, geheel of hoofdzakelijk bestaat uit het overbrengen van signalen via een elektronisch communicatienetwerk. Het begrip heeft een zeer breed bereik, waaronder ook internetdiensten en webgebaseerde e-maildiensten vallen. In het proces-verbaal 'omtrent de algemene functionaliteiten van Encrochat telefoons'32, is het volgende beschreven:

"Encro was een communicatieaanbieder van telefoons, waarmee middels de Encrochat applicatie versleutelde chats, bestaande uit tekstberichten en afbeeldingen, konden worden verzonden en ontvangen en waarmee onderling gebeld kon worden."

Er lijkt weinig twijfel mogelijk aan de conclusie dat Encrochat een elektronische communicatiedienst betreft.

Verplichting opgelegd aan de elektronische communicatiedienst?

Wat het OM in haar argumentatie voorts benoemt, wat ook relevant is voor de vraag of het onderhavige bewaren en gebruiken van de data valt binnen de werkingssfeer van richtlijn 2002/58, is dat het in de arresten van 6 oktober 2020 gaat om het opleggen van een verplichting aan elektronische communicatiediensten om gegevens te bewaren en te verwerken.

Met wat bekend is over de wijze waarop de informatie is verkregen, lijkt het hier namelijk niet zo te zijn dat Encro een verplichting is opgelegd om gegevens te bewaren en te delen. De betreffende autoriteiten hebben simpelweg ingebroken in het elektronisch communicatienetwerk, om zo zelf gegevens te bewaren en te verwerken. Is daarmee de werkingssfeer van richtlijn 2002/58 omzeild?

---

31 Rechtbank Amsterdam, 18 december 2020, ECLI:NL:RBAMS:2020:6443, pag. 4.
32 Proces-verbaalnummer LERDB20001-3905, opgemaakt op 10 september 2020.

Het is zo dat de arresten die hierboven zijn beschreven gaan over wetgeving, op basis waarvan maatregelen worden getroffen die een dergelijke verplichting bij elektronische communicatiediensten oplegt. In het La Qaudrature du Net-arrest gaat het ook over methodieken waarbij in ieder geval lijkt te zijn getracht om een dergelijke verplichting niet op te leggen, om op die manier de werkingssfeer van richtlijn 2002/58 te omzeilen. Paragraaf 103 van dit arrest lijkt hier van groot belang. Daarin is immers opgenomen dat wanneer staten zelf maatregelen treffen die afbreuk doen aan de regel dat elektronische communicatie vertrouwelijk is, zonder dat daarbij een verwerkingsverplichting op de betreffende diensten wordt opgelegd, de bescherming van de persoonsgegevens niet valt onder richtlijn 2002/58. In paragraaf 93 wordt bovendien overwogen dat uit art. 3 van de richtlijn blijkt dat de richtlijn van toepassing is op de verwerking van persoonsgegevens in verband met het aanbieden van openbare elektronische communicatiediensten. In het Ministerio Fiscal-arrest was reeds overwogen dat de richtlijn aldus dient te worden beschouwd als een regeling van de activiteiten van de verleners van dergelijke diensten.

De overwegingen lijken te leiden tot de conclusie dat het verwerken, bewaren en gebruiken van de Encrochatdata niet valt onder de werkingssfeer van richtlijn 2002/58. Toch stelt de verdediging zich primair op het standpunt dat het wel onder die werkingssfeer valt. Met de actie hebben de autoriteiten zich namelijk begeven op het terrein van de elektronische communicatiediensten. Ze hebben gedaan, wat in andere situaties een dergelijke dienst wordt verplicht te doen, waardoor het handelen valt binnen de werkingssfeer van de richtlijn. Wanneer wordt geoordeeld dat dit handelen niet valt onder deze werkingssfeer, dan zou dat de weg vrijmaken voor lidstaten om voortaan geen verplichtingen aan de elektronische communicatiediensten meer op te leggen, maar simpelweg in te breken in het netwerk om de data dan zelf te verzamelen. Het zou het nuttig effect van art. 15, lid 1, van de richtlijn ontnemen, zoals dat ook het geval zou zijn als men zou oordelen dat verplichtingen in het kader van een strafzaak, vanwege art. 1 lid 3 van de richtlijn, niet onder de werkingssfeer van de richtlijn zou vallen.

In verband met dit standpunt wordt ook nadrukkelijk acht geslagen op de doelstellingen, alsmede art. 5, lid 1 en 15, lid 1 van de richtlijn. Het doel van de richtlijn, zoals deze volgt uit art. 1 lid 1 daarvan, is het harmoniseren van “regelgeving van de lidstaten die nodig is om een gelijk niveau van fundamentele rechten en vrijheden – met name het recht op een persoonlijke levenssfeer – bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen […]”. Voorts wordt in art. 5 van de richtlijn overwogen dat lidstaten via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten. Zij verbieden met name het **afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie** en de daarmee verband houdende verkeersgegevens **door anderen dan gebruikers**, indien gebruikers daarmee niet hebben ingestemd, behoudens de uitzonderingen van art. 15, lid 1. Art. 15, lid 1, biedt lidstaten de mogelijkheid om wettelijke maatregelen te treffen om onder andere de reikwijdte van art. 5 te beperken. Het spreekt echter niet slechts van wettelijke maatregelen die een verplichting leggen op elektronische communicatiediensten. Het gaat over wettelijke maatregelen, waardoor het vertrouwelijke karakter van de communicatie en daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten, zonder toestemming van de gebruiker, wordt beperkt. Daar valt ook het onderhavige bewaren en gebruiken van de Encrochatdata onder.

Dat het onderhavige handelen valt binnen de werkingssfeer van richtlijn 2002/58, sluit overigens ook aan bij het standpunt dat het Centrum voor democratie en technologie innam in de La Quadrature du Net-zaak.

De verdediging stelt zich dan ook op het standpunt dat het bewaren en gebruiken van de Encrochatdata, zoals dat in Nederland gebeurt, valt binnen de werkingssfeer van richtlijn 2002/58 en dus het Unierecht. Daardoor dient dit bewaren en gebruiken te worden getoetst aan de bepalingen van die richtlijn, in het licht van de bepalingen als benoemd in het Handvest.

Wat als het niet valt onder de werkingssfeer van richtlijn 2002/58?

Als wordt geoordeeld dat het onderhavige handelen door de Nederlandse autoriteiten niet valt binnen de werkingssfeer van richtlijn 2002/58, is de vraag of het niet alsnog binnen de werkingssfeer van het Unierecht valt.

In verband met deze vraag wordt nogmaals acht geslagen op hetgeen het Hof overwoog in paragraaf 103 van het La Quadrature du Net-arrest. Daar wordt immers niet slechts overwogen dat wanneer staten zelf maatregelen treffen, zonder daarbij een verwerkingsverplichting op de elektronische communicatiedienst op te leggen, de bescherming van de betrokken gegevens niet valt onder richtlijn 2002/58. Ook wordt overwogen dat die bescherming dan valt onder het nationale recht, onderhevig aan de richtlijn 2016/680, waardoor de maatregelen dienen te voldoen aan het nationale constitutionele recht en het EVRM.

Richtlijn 2016/680 betreft de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, alsmede het vrije verkeer van die gegevens. Uit de preambule van die richtlijn blijkt dat wanneer de verwerking van de persoonsgegevens dit doel heeft, die richtlijn geldt. Wanneer er andere doelstellingen bestaan, geldt verordening 2016/679.

Ook wanneer de verwerking, bewaring en gebruikmaking van de Encrodata niet valt binnen de werkingssfeer van richtlijn 2002/58, valt het dus nog binnen de werkingssfeer van richtlijn 2016/680. Over de betekenis daarvan in het kader van de vraag naar de rechtmatigheid, wordt later in dit stuk stilgestaan.

Waar het hier om gaat, is de conclusie dat het bewaren en gebruiken van de Encrochatdata, valt binnen de werkingssfeer van het Unierecht.

Conclusie.

De conclusie van de verdediging is dat het bewaren en gebruiken van de Encrochatdata zoals dit door de Nederlandse autoriteiten wordt gedaan, valt binnen de werkingssfeer van het Unierecht. Primair stelt de verdediging zich op het standpunt dat het valt binnen de werkingssfeer van richtlijn 2002/58. Subsidiair stelt zij zich op het standpunt dat het valt binnen de werkingssfeer van richtlijn 2016/680.

Voorbereidend onderzoek en Schutznorm

In haar schrijven van 28 september 2020 legt het OM uit dat de Nederlandse autoriteiten geen bijdrage hebben geleverd aan het onderscheppen van de Encrochatdata. Vervolgens legt zij uit dat de data van de Franse autoriteiten zijn verkregen, binnen het kader van het onderzoek 26Lemont. Binnen dat onderzoek wordt de data bewaard en gebruikt. Als hieruit informatie voortkomt die van belang is voor andere strafzaken, dan wordt die informatie gedeeld, op grond van art. 126dd Sv. Daaraan kan het argument worden ontleend, dat wanneer het bewaren en gebruiken van de Encrochatdata onrechtmatig is, dit een onrechtmatigheid in een ander voorbereidend onderzoek betreft. In de zaak waarin de informatie vervolgens wordt verwerkt, zou die onrechtmatigheid niet kunnen worden beoordeeld op grond van art. 359a Sv. Daarvoor is immers van belang dat de onrechtmatigheid heeft plaatsgevonden in het betreffende voorbereidende onderzoek.

Moeilijk kan worden ontkend dat de constructie die door het OM wordt gehanteerd, gekunsteld overkomt. Onderzoek 26Lemont zou zich richten tegen Encrochat, waarbij de verdenking onder andere bestaat uit de medeplichtigheid aan strafbare feiten die door klanten van dat bedrijf werden of worden gepleegd.33

De vordering ex. art. 126uba Sv, die heeft geleid tot de machtiging, waardoor de Encrochatdata is onderzocht, is niet aan het dossier toegevoegd. Rechtbanken hebben tot op heden verzoeken om die vordering, met onderliggende processen-verbaal afgewezen. Dat is toch wel opmerkelijk, als men zich bedenkt dat er een redelijk vermoeden van schuld voor die medeplichtigheid dient te worden onderbouwd, waarbij ook acht dient te worden geslagen op het dubbel opzet. Moeilijk valt in te zien hoe het onderzoek bijdraagt aan het onderzoek naar die vermeende medeplichtigheid.

Deze opmerking is relevant, nu daaruit volgt dat niet kan worden gesteld dat de wijze waarop de Encrochatdata zijn bewaard en gebruikt, uiteindelijk zonder meer onderdeel gaat uitmaken van een rechterlijke toets binnen het kader van een inhoudelijke beoordeling van een strafzaak.

Bovendien, mocht dit wel het geval zijn, dan betreft dit een toets binnen het kader van het belang van Encrochat. Het is echter niet de privacy van Encrochat die wordt geschonden. Het is de privacy van de gebruikers van Encrochat, alsmede hun recht op de bescherming van de vertrouwelijkheid van hun communicatie en hun vrijheid van meningsuiting, waarop een inbreuk wordt gemaakt. De Schutznorm kan in het onderzoek 26Lemont er dan juist voor zorgen dat nader onderzoek of een inhoudelijk oordeel over de rechtmatigheid, achterwege blijft.

Het is juist die Schutznorm, bezien binnen een Unierechtelijk perspectief, dat de verdediging stelt dat de stelling dat het bewaren en gebruiken van de Encrochatdata plaatsvond in een ander voorbereidend onderzoek, niet kan leiden tot de conclusie dat de rechtmatigheid hiervan niet kan worden betrokken in de vragen van art. 348 en 350 Sv in de onderhavige zaak.

Als de verdediging in onderhavige zaak geen verweer kan voeren over de rechtmatigheid, dan ontbreekt het in de visie van de verdediging aan een effective remedy, als bepaald in art. 13 EVRM en art. 47 Handvest. Nu het OM haar verdenking onderbouwt met de informatie die is verkregen door het bewaren en gebruikmaken van de Encrochatdata, waarvan zojuist is vastgesteld dat dit binnen de werkingssfeer van het Unierecht valt, dient art. 359a Sv in dit verband evenzo conform het Unierecht te worden uitgelegd. Ook dit volgt uit het La Quadrature du Net-arrest. In die zaak werd de vraag gesteld wat er in strafzaken diende te gebeuren met de informatie die reeds was vergaard op basis van een onrechtmatige maatregel. Het Hof overwoog

33 Schrijven LP d.d. 28 september 2020, pag. 4

dat de lidstaten in dit verband zelf procedureregels dienen vast te stellen, waarbij geldt dat deze niet minder gunstig mogen zijn dan de regels over de beoordeling van onrechtmatigheden op basis van nationaal recht en de uitoefening van de door het Unierecht verleende rechten in praktijk niet onmogelijk of buitensporig moeilijk wordt gemaakt (effectiviteitsbeginsel). Dit effectiviteitsbeginsel, in verband met het recht op een daadwerkelijk rechtsmiddel, maakt in de visie van de verdediging dat het laten afketsen van een rechtmatigheidstoets op de stelling dat e.e.a. in een ander voorbereidend onderzoek is gedaan, in strijd is met het Unierecht.

Overigens wordt in dit verband ook nog acht geslagen op het Tele2-arrest, waarin ook wordt benoemd dat de rechtmatigheid van de maatregel, mede afhankelijk is van de vraag of de betreffende burger wordt geïnformeerd, zodat hij tegen de toepassing van de maatregel in beroep kan gaan.34

Hier is voorts nog een bespreking van een overweging van de rechtbank Rotterdam, in het onderzoek Flamenco, op zijn plaats. De rechtbank overwoog dat de beoordeling van onderzoekswensen wordt beïnvloed door de proceshouding van de verdachten. Een inhoudelijke verklaring, of het ontbreken daarvan, heeft volgens de rechtbank invloed op de vraag of een verzoek redelijkerwijs van belang is voor het nemen van een beslissing in het kader van de vragen van art. 348 en 350 Sv. De rechtbank heeft het dan concreet over een verklaring in verband met de gevoegde Encrochatinformatie. Zonder die verklaring kunnen onderzoekswensen “slechts” worden beoordeeld op basis van de rest van het dossier.35

Als het OM zich enkel en alleen op basis van Encrochatgegevens op het standpunt stelt dat de verdachte betrokken is bij het verweten strafbare feit, zoals in de onderhavige zaak het geval is, is een verklaring niet nodig om te concluderen dat onderzoek naar de rechtmatigheid van het bewaren en gebruiken van die gegevens redelijkerwijs van belang is voor het nemen van een beslissing in het kader van de vragen van art. 348 en 350 Sv. Het beroep op het zwijgrecht kan, al helemaal op dit punt in de procedure, niet leiden tot de conclusie dat onvoldoende is gebleken dat de verdachte in zijn belang is geschaad, waardoor nader onderzoek naar de rechtmatigheid achterwege kan blijven.

Tot slot, in verband met de vraag of de constatering dat het bewaren en gebruiken van de Encrochatdata plaatsvindt in een ander voorbereidend onderzoek, zij opgemerkt dat dit niet relevant is, wanneer de onrechtmatigheid een inbreuk maakt op het recht op een eerlijk proces van de verdachte. Ook overigens kan een onrechtmatigheid, zonder toepassing van art. 359a Sv, wel de daarin genoemde rechtsgevolgen hebben.36

Gelet op het voorgaande stelt de verdediging zich op het standpunt dat de constatering dat het bewaren en gebruiken van de Encrochatdata plaatsvond in het onderzoek 26Lemont, niet wegneemt dat de beoordeling van de rechtmatigheid in de onderhavige zaak redelijkerwijs van belang is voor de beantwoording van de vragen van art. 348 en 350 Sv.

34 HvJ EU, 21 december 2016, ECLI:EU:C:2016:970, Tele2, Par. 121.
35 Rechtbank Rotterdam, 25 januari 2021, ECLI:NL:RBROT:2021:396.
36 Conclusie AG F.W. Bleichrodt, 30 juni 2020, ECLI:NL:PHR:2020:655, par.. 95.

Bewaren en gebruiken van Encrochatdata is onrechtmatig.

Maakt het verschil of de maatregel valt binnen de werkingssfeer van richtlijn 2002/58 of richtlijn 2016/680?

De jurisprudentie die hierboven is besproken, geeft het kader op basis waarvan de verdediging zich op het standpunt stelt dat het bewaren en gebruiken van Encrochatdata onrechtmatig is. Die jurisprudentie is echter met name gewezen in verband met maatregelen die vallen binnen de werkingssfeer van richtlijn 2002/58. Het primaire standpunt van de verdediging is dat de onderhavige maatregelen ook binnen die werkingssfeer vallen. Wanneer echter wordt geoordeeld dat dit niet zo is, maar het valt binnen de werkingssfeer van richtlijn 2016/680, dan is de vraag of het juridisch kader dat in de voornoemde jurisprudentie is geschetst, nog wel geldt. De verdediging stelt zich op het standpunt dat dit wel zo is.

Ook wanneer de maatregelen vallen binnen de werkingssfeer van richtlijn 2016/680, dienen de bepalingen daarvan immers te worden uitgelegd tegen de achtergrond van het Handvest. Dat betekent dus dat, zoals ook volgt uit de voornoemde rechtspraak, de rechtmatigheid van de maatregelen afhankelijk is van de toelaatbaarheid van de inbreuken op de artikelen 7, 8 en 11 Handvest, beoordeeld in het licht van art. 52 Handvest, alsmede het evenredigheidsbeginsel. De algemene overwegingen die het Hof in dit verband heeft gemaakt, gelden hier dus ook.

Waar wel een duidelijk onderscheid bestaat, is dat uit art. 5 van richtlijn 2002/58 het uitgangspunt van de vertrouwelijkheid van elektronische communicatie wordt gedefinieerd, waarop op basis van art. 15 van de richtlijn een uitzondering kan worden gemaakt. Richtlijn 2016/680 benoemt dit uitgangspunt niet zo expliciet, hetgeen ook geldt voor de uitzondering. Desalniettemin kunnen het uitgangspunt en de uitzondering wel uit richtlijn 2016/680 worden afgeleid. In dat verband zij ook gewezen op paragraaf 26 in de preambule van de richtlijn:

"Iedere verwerking van persoonsgegevens dient ten aanzien van de natuurlijke personen in kwestie rechtmatig, behoorlijk en transparant te zijn en uitsluitend te geschieden met het oog op specifieke, bij wet vastgestelde doeleinden. […] Met name dienen de specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt expliciet en legitiem te zijn, en te worden vastgesteld op het ogenblik dat de persoonsgegevens worden verzameld. De persoonsgegevens moeten toereikend en ter zake dienend zijn voor de doeleinden waarvoor zij worden verwerkt. Meer bepaald moet ervoor worden gezorgd dat niet bovenmatig veel gegevens worden verzameld en dat zij niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij worden verwerkt. Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere manier kan worden verwezenlijkt. Om ervoor te zorgen dat gegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan."

Daarbij geldt dat deze richtlijn een veel bredere context heeft dan richtlijn 2002/58. Het ziet bijvoorbeeld ook op de opslag van een DNA-profiel. Het is dan ook niet gek dat de normen in richtlijn 2016/680 veel meer open zijn geformuleerd, dan in richtlijn 2002/58. De inhoud van de rechtmatigheidstoets die dient te worden aangelegd, is mede afhankelijk van de inbreuk die op grondrechten wordt gemaakt, zo blijkt ook uit paragraaf 37 van de preambule:

"Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden verdienen specifieke bescherming aangezien de context ervan aanzienlijke risico's voor de grondrechten en fundamentele vrijheden kan meebrengen."

Regelgeving in de richtlijn die in verband met het bovenstaande dient te worden beschouwd is allereerst art. 4, dat de beginselen inzake de gegevensverwerking voorschrijft. Uit lid 1, sub a, blijkt dat lidstaten dienen voor te schrijven dat persoonsgegevens rechtmatig en eerlijk worden verwerkt. Uit sub b blijkt voorts dat de verzameling geschiedt voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden en dat de verwerking niet plaatsvindt op een niet met die doeleinden te verenigen wijze. Bovendien dienen de persoonsgegevens volgens sub c toereikend, ter zake dienend en niet bovenmatig in verhouding tot de doeleinden waarvoor zij worden verwerkt, te zijn.

Voorts blijkt uit art. 5 van de richtlijn dat lidstaten voorzien in passende termijnen voor het wissen van de persoonsgegevens, of voor een periodieke evaluatie van de noodzaak van de opslag, waarbij de naleving van deze termijnen met procedurele maatregelen wordt gewaarborgd.

Tot slot zij hier nog gewezen op art. 8 lid 1, waaruit volgt dat de verwerking van persoonsgegevens alleen rechtmatig is indien dit noodzakelijk is voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het gebaseerd is op Unierecht of lidstatelijk recht.

Wanneer het gaat over de interpretatie van de voornoemde bepalingen, in het licht van de preambule van de richtlijn en tegen de achtergrond van het Handvest, kan het in de visie van de verdediging niet anders zijn dan dat de rechtmatigheidstoets hetzelfde is als die volgt uit richtlijn 2002/58. Het doel van de bepalingen in richtlijn 2002/58 is immers niet anders dan het doel van de bepalingen van richtlijn 2016/680, toegespitst op de onderhavige zaak. Het gaat om de bescherming van fundamentele rechten en vrijheden van de burger, meer specifiek zoals vastgelegd in de artikelen 7, 8 en 11 van het Handvest. Het zou afbreuk doen aan de daadwerkelijke bescherming van die rechten en vrijheden, als de reikwijdte van de bescherming niet afhankelijk is van de omvang van de inbreuk en het doel van de inbreuk, maar de methodiek die wordt gehanteerd. Heel concreet verwoord: niet valt uit te leggen dat de bescherming van vertrouwelijke communicatie van een burger verder gaat als een verplichting wordt opgelegd bij een elektronische communicatiedienst, dan wanneer een lidstaat inbreekt op het netwerk van een dergelijke dienst. Het past ook niet bij de doelstellingen van de Uniewetgever om een homogene bescherming van persoonsgegevens binnen de EU te garanderen.

Dat het toetsingskader niet anders is dan wanneer het binnen de werkingssfeer van richtlijn 2002/58 valt, blijkt overigens ook uit het Digital Rights-arrest. In dat arrest is de regelgeving die maatregelen mogelijk maakte om inbreuk te maken op de artikelen 7, 8 en 11 Handvest niet getoetst in het licht van art. 5 en 15 van richtlijn 2002/58. Het ging daar namelijk om de onverbindend verklaarde richtlijn 2006/24. Met name zij gewezen op de paragrafen 51 en 52 van het arrest. Die overwegingen sluiten naadloos aan bij het onderhavige standpunt.

Aldus stelt de verdediging zich op het standpunt dat wanneer wordt geoordeeld dat het bewaren en gebruiken van de Encrochatdata zoals dat in Nederland, meer specifiek in de onderhavige zaak gebeurt, niet valt binnen de werkingssfeer van richtlijn 2002/58, maar binnen de werkingssfeer van richtlijn 2016/680, de rechtmatigheidstoets niet anders is, dan wanneer het wel binnen de werkingssfeer van richtlijn 2002/58 zou vallen.

Omvang van de inbreuk op grondrechten

In de hiervoor besproken jurisprudentie is aan de orde gekomen op welke grondrechten en fundamentele vrijheden daar een inbreuk wordt gemaakt, alsmede de omvang daarvan. De maatregelen betreffen echter anderen dan in de onderhavige casus. Het is duidelijk geworden dat de wijze waarop de rechtmatigheidstoets plaatsvindt, afhankelijk is van de aard en omvang van de inbreuk op grondrechten en fundamentele vrijheden. Hier wordt stilgestaan bij die aard en omvang.

Om die aard en omvang te bepalen, dient acht te worden geslagen op de stukken die (officieel) vanuit 26Lemont zijn gedeeld, waaronder (het deel van) de machtiging van de rechter-commissaris en het proces-verbaal van bevindingen dat hij heeft opgemaakt.

Waar het gaat over de data die wordt bewaard, blijkt uit het proces-verbaal 'kaders gebruik dataset 26Lemont' welke data er wordt bewaard. *"Er is informatie van uitgewisselde chatberichten, alsmede informatie betreffende de contacten, notities en metadata van gebruikers van deze communicatiedienst verzameld"*.37

De data is met de Nederlandse autoriteiten gedeeld door de Franse autoriteiten. Nederlandse justitie kreeg een machtiging van de rechter-commissaris op 27 maart 2020, welke is verlengd op 28 april, 21 mei en 18 juni 2020 om data te vergaren die van de Franse autoriteiten werd verkregen.38 Wat is gedaan na verkrijging van de machtiging, blijkt uit het proces-verbaal 'overzicht beschikbare data Encrochat'.

Op vier momenten hebben de Franse autoriteiten kopieën gemaakt van de Encrochat infrastructuur. Dat is geweest in januari 2019, oktober 2019, februari 2020 en juni 2020. Dit wordt serverdata genoemd. Dit is toegevoegd aan het onderzoeksdossier van het JIT, dat in Nederland werkt onder de naam 26Lemont. Van 1 april 2020 tot en met 14 juni 2020 hebben de Fransen communicatie direct onderschept en verzameld. Dit wordt telefoondata genoemd. Ook dit is aan dat onderzoeksdossier toegevoegd. Beschreven wordt:

"Ten aanzien van de verkregen telefoondata geldt nog dat deze door de Franse autoriteiten is veiliggesteld onder de wettelijke kaders die in Frankrijk gelden op basis van een rechterlijke machtiging aldaar. Ten aanzien van die informatie [RP: dus niet de serverdata] *is daarnaast ook gezocht naar een rechterlijke toetsing binnen Nederland en heeft de rechter-commissaris in Rotterdam het Openbaar Ministerie gemachtigd kennis te nemen van de informatie afkomstig van telefoons die zich op Nederlands grondgebied bevonden binnen daarvoor gestelde kaders".39*

De bulkdata die door Frankrijk aan Nederland ter beschikking werd gesteld, werd op grond van de machtigingen in de periode waarvoor was gemachtigd, opgeslagen. Tot zover is de maatregel dus in tijd beperkt. Dat is echter niet het geval waar dit het bewaren en gebruiken van de vergaarde data betreft. Dat blijkt ook uit de navolgende overweging van de rechter-commissaris:

*"Per brief van 6 augustus 2020 is vervolgens aan de officier van justitie toestemming verleend de eerder met machtiging vergaarde data mogelijk ten behoeve van lopende of te starten strafrechtelijke onderzoeken te gebruiken, doch slechts onder de bij de initiële machtiging voorgestelde voorwaarden".*40

Op de inhoud van de voorwaarden zal later dieper worden ingegaan. Voor nu is het van belang om vast te stellen dat die voorwaarden er voor zorgen dat de vergaarde data onbeperkt bewaard kan blijven en deze ook ongelimiteerd kan worden doorzocht door middel van zoeksleutels die weliswaar goedgekeurd zijn door de rechter-commissaris, maar verder geheim worden gehouden. Wat we er wel van weten, is dat er zeer algemene zoektermen worden gebruikt, zoals pap, papier en loods. Ná het gebruik van de bewaarde data, kán de rechter-commissaris worden verzocht om de inhoud, omvang en de relatie tot vermoedelijk gepleegde strafbare feiten te controleren. Voor die controle, wordt de informatie niet ter beschikking gesteld aan het Openbaar Ministerie ten behoeve van (opsporings)onderzoeken. Als de betreffende autoriteiten vergaarde

37 Proces-verbaal 'kaders gebruik dataset 26Lemont', ongedateerd, opgemaakt door R225 en LAP0796.
38 Proces-verbaal van bevindingen van de rechter-commissaris, d.d. 20 september 2020, pag. 1-2.
39 Proces-verbaal 'overzicht beschikbare data Encrochat', d.d. 25 augustus 2020, pag. 4.
40 Proces-verbaal van bevindingen van de rechter-commissaris, d.d. pag. 2.

informatie niet willen gebruiken voor (opsporings)onderzoeken, wordt het dus niet door een rechter-commissaris gecontroleerd, terwijl de informatie om andere redenen dan een (opsporings)onderzoek dus wel kan worden gedeeld met opsporingsinstanties en het OM.

Daarbij dient te worden beseft dat dit dus slechts gaat over de 'telefoondata'. Het bewaren en gebruiken van de 'serverdata' gebeurt zonder enige grondslag of controle.

Gelet op het voorgaande geldt dat er sprake is van een inbreuk op de artikelen 7, 8 en 11 van het Handvest, die als zeer zwaar dient te worden aangemerkt. Er is sprake van een algemene en ongedifferentieerde set data, waarin niet alleen verkeers-, locatie- en persoonsgegevens zijn opgenomen, maar zelfs inhoudelijke communicatie. Die data set heeft geen houdbaarheidsdatum en kan onbeperkt worden gebruikt door de autoriteiten, terwijl er geen zicht is op wat er met de vergaarde data gebeurt, tenzij het wordt gebruikt voor een strafrechtelijk onderzoek, waarvoor dan een controle van de rechter-commissaris plaatsvindt.

De inbreuk op het recht op privéleven en de vertrouwelijkheid van communicatie, is evident. Door het opslaan en gebruiken van de onderhavige gegevens, is immers informatie voorhanden waaruit, in hun geheel beschouwd, zeer precieze conclusies kunnen worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.41

De verdediging stelt zich voorts op het standpunt, dat ook een inbreuk is gemaakt op de vrijheid van meningsuiting. De combinatie van de bewaarde gegevens, uiteraard met name de inhoud van de communicatie, kan een beeld geven van de wijze waarop communicatiemiddelen worden gebruikt en kan dus een beeld geven van de wijze waarop de vrijheid van meningsuiting wordt geëffectueerd.

Wettelijke grondslag.

Nu duidelijk is dat er sprake is van een inbreuk op de voornoemde grondrechten, is de vraag of dit, gelet op het bepaalde in art. 15 lid 1 richtlijn 2002/58, art. 52 lid 1 Handvest en het evenredigheidsbeginsel, als rechtmatig kan worden beoordeeld.

Het eerste vereiste in dat verband, dat zowel blijkt uit art. 15 lid 1 richtlijn 2002/58, als art. 52 lid 1 Handvest, is de wettelijke grondslag. Het Hof heeft in het Digital Rights-arrest overwogen dat de betrokken Unieregeling (maar dat geldt voor de nationale regeling niet anders), "duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens". Het geeft nog meer aanwijzingen over regelgeving. Het dient toepassing van de maatregel te beperken tot omschreven situaties, objectieve criteria ter begrenzing van de toegang van bevoegde nationale autoriteiten tot de gegevens te bevatten en materiële en procedurele voorwaarden te creëren betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. In het Tele2-arrest wordt hier nadere duiding aan gegeven. Ik verwijs naar het overzicht dat hiervan is gegeven op pagina 11 van dit stuk. Een onderdeel daarvan is het waard om nogmaals te belichten, namelijk dat de

41 Zie ook het Digital Rights-arrest, par. 27.

regelgeving objectieve criteria dient te stellen die een verband vereist tussen de te bewaren gegevens en het nagestreefde doel. De voorwaarde dient in praktijk van dien aard te zijn dat zij de omvang van de maatregel, en dus de kring van betrokken personen, daadwerkelijk afbakenen.

Als we het kader toepassen op de onderhavige casus, dan dient eerst te worden vastgesteld dat er twee verschillende typen data zijn, namelijk de serverdata en de telefoondata. De telefoondata is op basis van de machtigingen van de rechter-commissaris ex. art. 126uba jo. 126t Sv vergaard en opgeslagen. Een Nederlandse wettelijke grondslag voor de opslag van de serverdata is niet gegeven.

Dat leidt in ieder geval tot de visie dat het bewaren en gebruiken van de serverdata geen wettelijke grondslag heeft, waardoor de inbreuk die daardoor wordt gemaakt op de grondrechten van gebruikers, onrechtmatig is. Daarbij maakt het overigens geen verschil dat de betreffende data thans nog versleuteld is. Achter de versleuteling gaan immers dezelfde persoonsgegevens schuil, terwijl de nationale autoriteiten ten tijde het onrechtmatige bewaren juist proberen die versleuteling te doorbreken.

Het zijn hier echter niet de serverdata die onderdeel uitmaken van het dossier Finland. Het gaat hier om de telefoondata. Voor het verwerken en opslaan van die data, is dus een wettelijke grondslag gegeven, die wordt gevormd door art. 126uba jo. 126t Sv. De wettelijke bepalingen, kennen de volgende waarborgen:

- Er dient sprake te zijn van een verdenking van een georganiseerd verband, dat misdrijven beraamt of pleegt als genoemd in art. 67 lid 1 Sv, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren;
- Het onderzoek dient de maatregel dringend te vorderen;
- Er wordt ingebroken in een geautomatiseerd werk dat in gebruik is bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven;

Nu is een discussiepunt of met het verlenen van de machtiging is voldaan aan de waarborgen die bij die wet zijn gesteld. In dat verband is de discussie relevant of het onderzoek 26Lemont, met de verdenking die daar aan de orde is, dringend vordert dat alle communicatie wordt onderschept en onderzocht, alsmede of uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat alle gebruikers, waarvan de communicatie is onderschept, betrokken zijn bij het in georganiseerd verband beramen of plegen van misdrijven. Daarbij speelt ook de interpretatie van de ‘persoon die het geautomatiseerd werk in gebruik’ heeft een rol. Is dat Encrochat, of de gebruiker?

Eerste reflex hiertegen zal wellicht zijn dat dit vragen zijn die in het onderzoek 26Lemont aan de orde kunnen komen, maar niet relevant zijn voor het onderzoek Finland. De visie van de verdediging is echter anders. Als immers de conclusie is dat de persoon die het geautomatiseerd werk in gebruik heeft niet Encrochat is, maar de gebruiker van het communicatiemiddel (wat een vrij logische conclusie is), dan is de conclusie op basis van art. 126uba dat voor het toepassen van de maatregel een redelijk vermoeden bestaat dat die gebruiker betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven. Dat leidt dus tot de conclusie dat de visie van het OM moet zijn dat iedere gebruiker van Encrochat daar inderdaad van wordt verdacht, wat de vraag doet rijzen of dat uit voldoende feiten en omstandigheden blijkt. De visie van de rechter-commissaris is in ieder geval geweest dat art. 126ubo Sv voldoet. De visie van de verdediging is anders.

Het is echter niet slechts een discussie van nationaal recht of deze interpretatie juist is, maar ook een Unierechtelijke discussie. Art. 126uba dient immers conform het Unierecht te worden geïnterpreteerd, waarbij juist ook de bescherming van de grondrechten van de personen die door de maatregelen worden getroffen, centraal staat.

Daarbij komt ook het punt van de onbeperkte houdbaarheid van de dataset. De machtiging van de rechter-commissaris was natuurlijk telkens voor een bepaalde termijn gegeven, maar de termijn die ook wordt voorgeschreven in art. 126uba lid 2 sub g Sv, ziet op het vergaren van de informatie. Nu is er een enorme bulk aan algemene en ongedifferentieerde data vergaard, maar op grond van art. 126uba Sv wordt niets bepaald over de termijn dat deze mag worden bewaard. Dit, terwijl juist uit de hiervoor besproken jurisprudentie blijkt, dat het bewaren en gebruiken van data niet langer mag duren, of verder mag gaan, dan strikt noodzakelijk.

Het standpunt van de verdediging is aldus dat 126uba Sv onvoldoende grondslag biedt voor het bewaren en gebruiken van de data zoals gebeurt en ook in onderzoek Finland is gebeurd.

Evenredigheidsbeginsel

Indien wordt geoordeeld dat er een wettelijke grondslag bestaat voor het verwerken, opslaan, bewaren en gebruiken van de data, dan is de vraag of daarmee ook wordt voldaan aan het evenredigheidsbeginsel. De verdediging stelt zich op het standpunt dat dit niet zo is. Hiervoor wordt wederom acht geslagen op het Digital Rights-arrest, waaruit blijkt dat de toets van de noodzaak, die uit dit evenredigheidsbeginsel voortvloeit, inhoudt dat uitzonderingen op de bescherming van de vertrouwelijke communicatie, beperkt dient te worden binnen de grenzen van het strikt noodzakelijke. Een dergelijke toets past bij een doelstelling die de Uniewetgever ook had bij het creëren van richtlijn 2002/58, te weten het bieden van “een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronische communicatiediensten, ongeacht de gebruikte technologie”, waaraan ook in het Tele2-arrest werd gememoreerd.

Vastgesteld is dat er sprake is van een algemene en ongedifferentieerde bewaring van de Encrochatdata. Het bewaren van die data vormt een grotere inbreuk op de rechten als genoemd in de artt. 7, 8 en 11 Handvest, omdat het hier ook om inhoudelijke communicatie gaat. Niet kan worden volgehouden dat het bewaren van deze gegevens strikt noodzakelijk is, omdat voor een groot deel, maar toch in ieder geval in de onderhavige zaak, helemaal geen verdenking bestond op basis waarvan kon worden geoordeeld dat er een noodzaak bestond om in de Encrochatdata te zoeken, laat staan dat het strikt noodzakelijk was. Uiteraard was in het onderzoek Finland reeds duidelijk dat er sprake was van een misdrijf, maar uit de betreffende bevindingen bleek niet een verband met Encrochatdata of specifieke gebruikers daarvan.

Geconcludeerd dient aldus te worden dat de doelstelling van het zoeken in de Encrochatdata, dat heeft geleid tot de informatievergaring die in de onderhavige zaak wordt gebruikt, was het opsporen van misdrijven, in het algemeen.

Die vaststelling onderschrijft de conclusie dat niet is voldaan aan het vereiste dat het bewaren en gebruiken van de data strikt noodzakelijk dient te zijn. Ook in dit verband zij weer gewezen op het Tele2-arrest, meer specifiek paragraaf 103, waarin het hof overwoog:

“Daarbij komt dat de doeltreffendheid van de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een nationale regeling die

voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens, noodzakelijk wordt geacht voor het voeren van deze strijd."

Daarbij moet wel worden toegegeven dat, zo kan men wel aannemen, het aantal gebruikers van Encrochat aanzienlijk minder is dan het aantal gebruikers van een telecomprovider, zoals Tele2. Dit besef plaatst het woord "alle" in de hierboven geciteerde paragraaf, wel in een ander perspectief. Dat brengt mij weer bij de overwegingen in het La Quadrature du Net-arrest. In dat arrest werd weliswaar herhaald dat de bestrijding van ernstige criminaliteit, nooit wetgeving legitimeert die de algemene en ongedifferentieerde opslag van verkeers- en locatiegegevens mogelijk maakt, maar ook werd overwogen dat het wel legitiem kan zijn als de grens van een dergelijke maatregel onder andere wordt bepaald door bijvoorbeeld een geografisch criterium.

Benoemd werd dat wanneer is gebleken van plaatsen waar een hoog risico bestaat van voorbereiding of het plegen van ernstige strafbare feiten, of die daar extra gevoelig voor zijn, daar wel vergaande maatregelen kunnen worden getroffen. Men zou een vergelijk kunnen trekken met Encrochat. De stelling dat er een verhoogd risico bestaat, juist doordat er gebruik wordt gemaakt van Encrochat, wat een veelgebruikt medium zou zijn om te communiceren over misdrijven, kan leiden tot een afbakening op basis waarvan de stelling kan worden geformuleerd, dat de algemene en ongedifferentieerde verzameling, bewaring en gebruikmaking van de Encrochatdata wel is gerechtvaardigd, in het licht van het doel dat wordt nagestreefd.

Wanneer die stelling zou worden ingenomen, zou voorbij worden gegaan aan het feit dat uit de jurisprudentie ook volgt dat er voorafgaand aan de inzet van de maatregel op objectieve gronden is gekomen tot een redelijk vermoeden dat er ernstige misdrijven worden beraamd of gepleegd, waardoor de handeling ten aanzien van de concrete gebruikers is gerechtvaardigd. Voorts miskent het de overweging van het Hof dat ook in dit geval, toepassing van de maatregel dient te worden beperkt tot het strikt noodzakelijke. Juist door het gebruik van zeer algemene zoeksleutels, zonder een voorafgaande concrete verdenking, terwijl de bewaring en het gebruik niet is gelimiteerd in tijd, kan niet worden geoordeeld dat aan dat proportionaliteitsvereiste is voldaan. Een overweging als genoemd in de vorige alinea, kan derhalve ook niet in de weg staan aan het oordeel dat het bewaren en gebruiken van de Encrochatdata, zoals dat ook in onderhavige zaak is gebeurd, onrechtmatig is.

Het bovenstaande leidt tot de conclusie dat als er sprake is van een wettelijke grondslag voor het bewaren en gebruiken van de Encrochatdata, deze, of in ieder geval de toepassing zich niet verhoudt met het evenredigheidsbeginsel, zoals dit voortvloeit uit art. 52 Handvest.

Conclusie over de rechtmatigheid.

Al het voorgaande brengt de verdediging tot de conclusie dat het bewaren en gebruiken van de Encrochatdata dat heeft geleid tot het verkrijgen van de informatie die is gevoegd in het dossier Finland en als belastend bewijs jegens cliënt wordt gepresenteerd, onrechtmatig is.

De handelingen ontberen een wettelijke grondslag, of, voor zover deze dat wel hebben, verhoudt de wettelijke grondslag, of de interpretatie ervan die hier ten grondslag ligt aan het handelen, zich niet met de interpretatie, die conform art. 15 lid 1 richtlijn 2002/58, dan wel de artikelen 4, 5 en 8 van richtlijn 2016/680, gelezen tegen de achtergrond van de artikelen 7, 8, 11 en 52 van het Handvest, had dienen plaats te vinden.

Die onrechtmatigheid is, ondanks dat het vergaren van de Encrochatdata formeel heeft plaatsgevonden in het onderzoek 26Lemont, van belang voor de beoordeling van de vragen van de artikelen 348 en 350 Sv in de onderhavige zaak. Het beperken van de rechtmatigheidstoets tot in de zaak 26Lemont, waarvan überhaupt de vraag is of die ooit door een rechtbank inhoudelijk wordt getoetst, is in strijd met recht op een effectief rechtsmiddel, nu met de maatregel juist inbreuk wordt gemaakt op de communicatie van de gebruikers van Encrochat. Volgens het OM is cliënt gebruiker van Encrochat, hetgeen volledig ten grondslag ligt aan de verdenking en daarmee ook de voorlopige hechtenis, waardoor aan hem ook het recht toekomt om de rechtmatigheid te laten toetsen. Artikel 359a Sv dient daarom normconform te worden geïnterpreteerd, waardoor het vereiste dat de onrechtmatigheid in het voorbereidend onderzoek van de betreffende zaak dient te hebben plaatsgevonden, niet kan worden gevolgd.

Voor zover toch wordt geoordeeld dat het feit dat het bewaren en gebruiken van de data formeel niet in dit voorbereidend onderzoek heeft plaatsgevonden, in de weg staat aan toepassing van art. 359a Sv, dan geldt dat het verbinden van een rechtsgevolg aan een onrechtmatigheid niet slechts kan op grond van art. 359a Sv. Ook hier geldt weer dat het Unierecht de verplichting aan de lidstaat oplegt om te acteren op handelingen van de nationale autoriteiten, die in strijd zijn met het Unierecht, maar waarvan de resultaten worden betrokken in een strafzaak.

Gelet op de verplichting om te reageren op de onrechtmatigheid, vanwege het Unierecht, gecombineerd met het feit dat het hier een zeer vergaande inbreuk op het recht op privacy en het recht op vertrouwelijke communicatie betreft, die voorts ook van invloed is op de vrijheid van meningsuiting en het feit dat deze onrechtmatige inzet een zeer grote invloed heeft op de opsporing en vervolging van strafbare feiten in Nederland, is een daadwerkelijke reactie van groot belang. In dat verband zij ook gewezen op de overwegingen van de Hoge Raad in r.o. 2.4.5 in het ‘onbevoegde hulpofficier’-arrest, van 19 februari 2013.42

42 HR 19 februari 2013, ECLI:NL:HR:2013:BY5321

Prejudiciële vragen.

In de conclusie die hierboven is gegeven is (uiteraard) nog niet uitputtend beschreven, wat de visie van de verdediging is, over de rechtsgevolgen die het onrechtmatige bewaren en gebruiken van de Encrochatdata dienen te hebben. Dat zal op de inhoudelijke behandeling worden beargumenteerd.

Hier gaat het om de argumentatie van de verdediging waarom voornoemd handelen onrechtmatig is en waarom dit van belang is voor de te beantwoorden van vragen van art. 348 en 350 Sv in de onderhavige zaak. Die argumentatie is van belang voor de beoordeling van het verzoek dat het doel is van onderhavig stuk. Het stellen van prejudiciële vragen aan het Hof van Justitie van de Europese Unie.

Juridisch kader

Een dergelijk verzoek kan worden gedaan op grond van art. 267 VWEU. In dit artikel is genoemd dat het Hof een prejudiciële beslissing kan nemen, indien een vraag te dien aanzien wordt opgeworpen door een rechtelijke instantie, wanneer zij een beslissing op dit punt noodzakelijk acht voor het wijzen van haar vonnis.

Over de interpretatie van art. 267 VWEU is door het Hof het CILFIT-arrest gewezen, dat weliswaar met name van belang is in de zaken waar geen beroep mogelijk is, maar welke overwegingen ook van belang zijn voor de beoordeling van de noodzaak. AG Spronken heeft de betekenis van dit arrest, voor de gevallen waarin beroep mogelijk is en de rechter gehouden is prejudiciële vragen te stellen, samengevat:

“Gelet op het CILFIT-arrest van het HvJ EU vervalt de verplichting tot het stellen van prejudiciële vragen als de rechter heeft vastgesteld dat de betreffende Uniebepaling al door het HvJ EU in een vrijwel identiek geval is uitgelegd of de juiste uitleg rechtstreeks uit zijn jurisprudentie kan worden afgeleid (acte éclairé), of de toepassing van gemeenschapsrecht “zo evident” is, “dat redelijkerwijs geen ruimte voor twijfel kan bestaan” omtrent de wijze waarop de gestelde vraag moet worden opgelost (acte clair). Oftewel, zoals de Hoge Raad dat zelf formuleerde: van het stellen van prejudiciële vragen kan worden afgezien indien i) de opgeworpen prejudiciële vragen niet relevant zijn voor de oplossing van het geschil, dan wel ii) deze kunnen worden beantwoord aan de hand van de rechtspraak van het Hof van Justitie, of iii) dat redelijkerwijs geen twijfel kan bestaan over de wijze waarop deze vragen over de betrokken Unierechtelijke rechtsregel moeten worden opgelost. Het HvJ EU legt in genoemd CILFIT-arrest de lat hoog: alleen in het geval dat de nationale rechter ervan overtuigd is dat de beantwoording van de vraag even evident zou zijn voor de rechterlijke instanties van de andere Lidstaten als voor het HvJ EU, kan hij ervan afzien om de vraag voor te leggen aan het HvJ EU en ze op eigen verantwoordelijkheid oplossen. Het bestaan van acte clair mag dus niet al te snel worden aangenomen en er moet volgens het CILFIT-arrest rekening worden gehouden met de verschillende taalversies van het Verdrag, de eigen terminologie van het Europese recht en de context van de bepaling waar het om gaat. Het EHRM heeft bovendien het belang van het stellen van prejudiciële vragen onderstreept door het ongemotiveerd voorbijgaan aan een verzoek daartoe in strijd te achten met het recht op een eerlijk proces”.43

43 AG Spronken, 22 december 2015, ECLI:NL:PHR:2015:2710.

De noodzaak

Gelet op het juridisch kader, kan in de visie van de verdediging niet anders worden geconcludeerd dan dat:

1. De interpretatie van de betrokken Unierechtelijke bepalingen van relevant is voor de beoordeling van de vragen van art. 348 en 350 Sv;
2. Er geen sprake is van een acte éclairé;
3. Er geen sprake is van een acte clair.

De noodzaak wordt voorts nader onderbouwd door het feit, dat de beantwoording van de vragen van doorslaggevend belang is voor de beoordeling van de onderhavige strafzaak. De belastende bewijsmiddelen jegens cliënt worden uitsluitend gevormd door de Encrochatdata.

Het behelst bovendien rechtsvragen waarover niet eerder in de Nederlandse jurisprudentie inhoudelijk is beslist, terwijl de beslissingen op onderzoekswensen die er thans liggen en ingaan op het Unierecht, daar een evident onjuiste uitleg van geven.

Er is bovendien een zaaksoverstijgend belang wat de noodzaak tot het stellen van prejudiciële vragen vergroot. Veel strafzaken, waarin grote belangen op het spel staan, worden beheerst door de Encrochatdata en daarmee ook de rechtmatigheid ervan. Vanuit het oogpunt van rechtszekerheid, maar ook een efficiënte rechtsbedeling, is het noodzakelijk om zo spoedig mogelijk helderheid te krijgen over de rechtmatigheid van het bewaren en gebruiken van de Encrochatdata, in het licht van zowel de visie van het OM, als het standpunt van de verdediging, zoals dat hierboven is verwoord. De standpunten die hierboven zijn ingenomen, zullen naar verwachting niet slechts in deze zaak worden ingenomen. Wanneer het Hof de standpunten reeds nu beoordeelt, door beantwoording van de prejudiciële vragen, wordt daarmee voorkomen dat door rechtbanken en gerechtshoven in het hele land, telkens op dit onderwerp dient te worden besloten, om vervolgens bij de Hoge Raad te komen, waar een nieuw toetsingskader geldt voor de beoordeling van het verzoek om prejudiciële vragen, en in potentie de situatie kan ontstaan dat vele zaken opnieuw dienen te worden beoordeeld.

De vragen die de verdediging op grond van al het voornoemde voorstelt, zijn de navolgende.

Prejudiciële vragen

1. Valt het bewaren en gebruiken van de Encrochatdata zoals dit in Nederland gebeurt, binnen de werkingssfeer van 2002/58?
    a. Zo nee, valt het binnen de werkingssfeer van richtlijn 2016/680?
    b. Zo nee, valt het overigens binnen de werkingssfeer van het Unierecht?
2. Wordt met het bewaren en gebruiken van de Encrochatdata zoals dit in Nederland gebeurt, inbreuk gemaakt op de artikelen 7, 8 en 11 van het Handvest?
3. Als het valt binnen de werkingssfeer van richtlijn 2016/680 of overig Unierecht, wijkt de rechtmatigheidstoets van de inbreuk op de rechten als vervat in de artikelen 7, 8 en 11 van het Handvest dan af van de kaders die zijn geschetst in de jurisprudentie over de interpretatie van art. 5 en 15 van richtlijn 2002/58, zoals laatstelijk besproken in het arrest La Quadrature du Net?
4. Biedt artikel 126uba Sv de wettelijke grondslag, die vanwege art. 15 lid 1 richtlijn 2002/58 en art. 52 lid 1 Handvest noodzakelijk is voor een rechtmatige beperking van de grondrechten, zoals hier aan de orde?
    a. Zo ja, voldoet de wettelijke grondslag aan de eisen die voortvloeien uit art. 15 lid 1 richtlijn 2002/58 en art. 52 lid 1 Handvest?

5. Indien de onderhavige maatregel een wettelijke grondslag heeft, voldoet deze dan aan de vereisten die voortvloeien uit het evenredigheidsbeginsel?
6. Indien wordt geoordeeld dat de toepassing van de maatregel in strijd is met het Unierecht, staat het recht van een effectief rechtsmiddel, als genoemd in art. 47 Handvest, alsmede het effectiviteitsbeginsel als genoemd in het La Quadrature du Net-arrest, dan in de weg aan het oordeel dat de rechtmatigheid niet wordt beoordeeld in de strafzaak waarin de gebruikte informatie wordt betrokken, omdat het in een andere strafzaak is verwerkt?