Datum van inontvangstneming	:	13/06/2022

Geanonimiseerde versie

Zaak C-241/22

Verzoek om een prejudiciële beslissing

Datum van indiening:

6 april 2022

Verwijzende rechter:

Hoge Raad der Nederlanden (Nederland)

Datum van de verwijzingsbeslissing:

5 april 2022

Verzoekende partij:

Advocaat-generaal bij de Hoge Raad der Nederlanden

HOGE RAAD DER NEDERLANDEN

STRAFKAMER

[OMISSIS]

Datum 5 april 2022

ARREST

op het beroep in cassatie in het belang der wet van de advocaat-generaal bij de Hoge Raad der Nederlanden tegen een beschikking van [de] rechtbank Gelderland van 15 september 2021, [OMISSIS] in de zaak

van

DX,

[OMISSIS] hierna: de verdachte.

1. De beschikking van de rechtbank [Gelderland]

De rechtbank heeft de beschikking van de rechter-commissaris, waarbij de vordering van de officier van justitie dat de rechter-commissaris een machtiging verleent voor het vorderen van de verstrekking van historische verkeersgegevens is afgewezen, vernietigd en heeft deze vordering alsnog toegewezen.

2. Het cassatieberoep

De advocaat-generaal B.F. Keulen heeft beroep in cassatie in het belang van de wet ingesteld. De voordracht tot cassatie is aan dit arrest gehecht en maakt daarvan deel uit. De vordering strekt tot schorsing van de behandeling van het cassatieberoep teneinde prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie over de uitleg van artikel 15 lid 1 van Richtlijn 2002/58/EG, althans tot vernietiging van de beschikking van de rechtbank.

3. Waar het in deze zaak om gaat

De advocaat-generaal constateert in zijn vordering dat in de praktijk onduidelijkheid is ontstaan over, kort gezegd, de toepassingsvoorwaarden voor het doen van een vordering door de officier van justitie om verkeers- en locatiegegevens van een gebruiker van een communicatiedienst te verstrekken. Het gaat daarbij in het bijzonder om de vraag welke eisen voortvloeien uit Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie; hierna: Richtlijn 2002/58/EG),[1] en de rechtspraak van het Hof van Justitie van de Europese Unie (hierna: Hof van Justitie) over deze richtlijn. In zijn vordering bespreekt de advocaat-generaal een aantal vragen over de consequenties van Richtlijn 2002/58/EG en de rechtspraak van het Hof van Justitie voor de toepassing van het Nederlandse strafprocesrecht, en legt die vragen voor aan de Hoge Raad aan de hand van de beschikking van de rechtbank en twee beschikkingen van een rechter-commissaris. Deze laatstgenoemde beschikkingen komen aan de orde in de zaken onder 21/04309 CW (ECLI:NL:HR:2022:476) en 21/04311 CW (ECLI:NL:HR:2022:477).

[OMISSIS]

4. De overwegingen van de rechtbank

4.1 De beschikking van de rechtbank is gegeven op het hoger beroep dat de officier van justitie heeft ingesteld tegen de afwijzing van een vordering tot het verlenen van een schriftelijke machtiging voor het vorderen van

[1] PbEU 2002, L 201/37; gewijzigd door Richtlijn 2009/136/EG, PbEU 2009, L 337/11.

historische/toekomstige gegevens als bedoeld in artikel 126n lid 1 van het Wetboek van Strafvordering. [OMISSIS]

[OMISSIS]

[OMISSIS] [de inhoud van de beslissing van de rechter-commissaris is weergegeven in punt 4.2]

4.2 De rechtbank heeft de beschikking van de rechter-commissaris vernietigd en de vordering van de officier van justitie toegewezen. De beschikking van de rechtbank luidt als volgt:

"[OMISSIS]

De vordering [van de officier van justitie] heeft betrekking op gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker, welke gebruiker kan worden geduid met "DX". Het betreft gegevens ten aanzien van Nederlands telefoonnummer mobiel alleen spraak: 316(...), over de periode van 9 augustus 2021 tot en met 12 augustus 2021.

[OMISSIS]

[OMISSIS] [procedure]

Oordeel van de rechter-commissaris

De rechter-commissaris heeft aan haar afwijzende beslissing ten grondslag gelegd dat uit het Prokuratuur-arrest van het Hof van Justitie van de Europese Unie (ECLI:EU:C:2021:152), volgt dat de toegang tot gegevens waarop de vordering betrekking heeft, alleen is toegestaan in procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid. In de Nederlandse context kan hiervoor aansluiting worden gezocht bij het criterium dat het gaat om verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Daarnaast moet de inzet van het opsporingsmiddel proportioneel en subsidiair zijn. De rechter-commissaris is van oordeel dat de onderhavige vordering moet worden afgewezen omdat het feit, de diefstal van een shovel, naar zijn aard geen ernstige inbreuk op de rechtsorde oplevert en dat bovendien niet gebleken is van enige samenhang met andere (door de verdachte) begane misdrijven.

Standpunt van de officier van justitie

Het hoger beroep strekt ertoe dat de beslissing van de rechter-commissaris wordt vernietigd. De officier van justitie stelt zich op het standpunt dat de rechter-commissaris een onjuiste maatstaf toepast bij de vraag of sprake is van “serious crime”, zoals genoemd in het Prokuratuur-arrest. De gehanteerde maatstaf is naar het oordeel van de officier van justitie (veel) te zwaar bij de beoordeling als bedoeld in artikel 126n en 126ng Sv. Dat betreffen voor verdachte relatief weinig ingrijpende bijzondere opsporingsbevoegdheden afgezet tegen meer ingrijpende bevoegdheden, zoals een telefoontap. Door die strenge maatstaf aan te leggen bij de beoordeling van de gevorderde machtiging wijkt de rechter-commissaris af van de beslissing die de wetgever heeft verbonden aan het verkrijgen van verkeers- en/of locatiegegevens als bedoeld in artikel 126n en 126ng Sv. Reeds het gegeven dat op het feit dat verdachte wordt verweten een maximale gevangenisstraf is gesteld van 6 jaren en dat voor dit feit toepassing van de voorlopige hechtenis mogelijk is, maakt naar het oordeel van de officier van justitie dat kan worden gesproken van een “serious crime” in de zin van het Prokuratuur-arrest. Bovendien heeft de raadkamer de gevangenhouding bevolen voor 90 dagen op grond van de grote recidivegrond. Het feit dat verdachte wordt verweten brengt een gewichtige reden van maatschappelijke veiligheid met zich mee die onverwijlde vrijheidsneming vordert. Die omstandigheid maakt naar het oordeel van de officier van justitie des te meer dat het feit dat verdachte wordt verweten zonder meer heeft te gelden als een “serious crime” in de zin van het Prokuratuur-arrest.

Ontvankelijkheid

[OMISSIS] [ontvankelijkheid van de vordering van de officier van justitie]

Beoordeling

De raadkamer stelt - in lijn met hetgeen door de Rotterdamse rechtbank is overwogen in het vonnis van 30 april 2021 (ECLI:NL:RBROT:2021:3906) - voorop dat uit het arrest van het Hof van Justitie EU H.K. vs. Estland (Prokuratuur) (ECLI:EU:C:2021:152) onder meer volgt dat het voor strafrechtelijke doeleinden verlenen van toegang tot de in het arrest bedoelde communicatiegegevens, te weten verkeers- en locatiegegevens, slechts is toegestaan in het kader van procedures ter bestrijding van zware criminaliteit en procedures ter voorkoming van ernstige bedreigingen van de openbare veiligheid. Het gaat hier immers om een ernstige inmenging op de grondrechten van artikel 7 en 8 EU-Handvest waarbij uit de opgevraagde persoonsgegevens nauwkeurige conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkene.

Aldus moet eerst worden bezien of het opvragen van de betreffende gegevens in de onderhavige zaak plaats vond in het kader van een procedure ter bestrijding van zware criminaliteit. De raadkamer is van oordeel dat die vraag bevestigend moet worden beantwoord. De vordering is gedaan in het kader van een strafrechtelijk onderzoek naar een gekwalificeerde diefstal door twee of meer personen van een goed met een waarde van circa € 18.000,-. Dit is een strafbaar feit waarop een maximale gevangenisstraf van zes jaar is gesteld en waarvoor voorlopige hechtenis is toegelaten (tegen verdachte is ook een bevel bewaring verleend) en dat een ernstige inbreuk maakt op de rechtsorde.

Gelet op het vorenstaande zal de beschikking van de rechter-commissaris worden vernietigd en de vordering van de officier van justitie alsnog worden toegewezen.

[OMISSIS]

5. Juridisch kader

Wetboek van Strafvordering

5.1.1 In het Wetboek van Strafvordering (hierna: Sv) wordt aan de officier van justitie de bevoegdheid toegekend om in het belang van het onderzoek een vordering te doen (historische en/of toekomstige) gegevens te verstrekken over (i) een gebruiker van een communicatiedienst en (ii) het communicatieverkeer met betrekking tot die gebruiker. Het gaat daarbij om zogenoemde verkeers- en locatiegegevens. Dat zijn onder meer gegevens met betrekking tot verbindingen die door of met de gebruiker tot stand zijn gebracht, en de locatiegegevens van een netwerkaansluitpunt of gegevens over de geografische positie van de randapparatuur van een gebruiker in het geval van een verbinding of een poging daartoe.[2] Daarnaast heeft de officier van justitie de bevoegdheid om te vorderen dat identificerende gegevens worden verstrekt, dat wil zeggen: gegevens ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. De hier genoemde vorderingen kunnen worden gericht tot iedere aanbieder van een communicatiedienst.

5.1.2 Deze bevoegdheden zijn allereerst neergelegd in artikel 126n en 126na Sv.

Artikel 126n Sv luidt:

> “1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een

[2] Zie nader artikel 2 van het onder 5.3 geciteerde Besluit vorderen gegevens telecommunicatie.

gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker. De vordering kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:

a. ten tijde van de vordering zijn verwerkt, dan wel

b. na het tijdstip van de vordering worden verwerkt.

2. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een communicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing. Indien de vordering, bedoeld in het eerste lid, betrekking heeft op een persoon die aanspraak kan maken op bronbescherming, kan deze slechts worden gedaan na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 218a, tweede lid, is van overeenkomstige toepassing.

3. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering gedaan voor een periode van ten hoogste drie maanden.

4. De officier van justitie doet van de vordering proces-verbaal opmaken, waarin worden vermeld:

a. het misdrijf en, indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;

b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, eerste volzin, zijn vervuld;

c. indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon omtrent wie gegevens worden gevorderd;

d. de gegevens die worden gevorderd;

e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, de periode waarover de vordering zich uitstrekt.

5. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in het eerste lid, eerste volzin. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering doet de officier van justitie proces-verbaal opmaken.

6. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de officier van justitie worden gevorderd.

Artikel 67 lid 1 Sv, waarnaar in artikel 126n Sv wordt verwezen, luidt:

"Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van:

a. een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld;

b. een der misdrijven omschreven in de artikelen 132, 138a, 138aa, 138ab, 138b, 138c, 139c, 139d, eerste en tweede lid, artikel 139h, eerste en tweede lid, 139g, 140, tweede lid, 141a, 137c, tweede lid, 137d, eerste lid, 137e, tweede lid, 137g, tweede lid, 151, 184a, 254a, 248d, 248e, 272, 284, eerste lid, 285, eerste lid, 285b, 285c, 300, eerste lid, 321,326c, tweede lid, 326d, 340, 342, 344a, 344b, 347, eerste lid, 350, 350a, 350c, 350d351,395, 417bis, 420bis.1,420quater en 420quater.1 van het Wetboek van Strafrecht;

c. een der misdrijven omschreven in:

artikel 86i, eerste lid, van de Elektriciteitswet 1998;

artikel 66h, eerste lid, van de Gaswet;

artikel 8.12, eerste en tweede lid, van de Wet dieren;

de artikelen 175, tweede lid, onderdeel b, of derde lid in verbinding met het eerste lid, onderdeel b en 176, tweede lid, voor zover dit betreft artikel 7, eerste lid, onderdelen a en c, van de Wegenverkeerswet 1994;

artikel 30, tweede lid, van de Wet buitengewone bevoegdheden burgerlijk gezag;

de artikelen 52, 53, eerste lid en 54 van de Wet gewetensbezwaren militaire dienst;

artikel 36 van de Wet op de kansspelen;

de artikelen 11, tweede lid, en 11 a van de Opiumwet;

artikel 55, tweede lid, van de Wet wapens en munitie;

artikel 11 van de Wet tijdelijk huisverbod;

artikel 8 van de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding.”

Artikel 126na Sv luidt:

“1. In geval van verdenking van een misdrijf kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Artikel 126n, tweede lid, is van toepassing.

2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126m of artikel 126n kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt.

3. In geval van een vordering als bedoeld in het eerste of tweede lid is artikel 126n, vierde lid, onder a, b, c en d, van overeenkomstige toepassing en blijft artikel 126bb buiten toepassing.

4. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de opsporingsambtenaar of de officier van justitie worden gevorderd.”

De termen “aanbieder van een communicatiedienst” en “gebruiker van een communicatiedienst” in deze bepalingen zijn gedefinieerd in artikel 138g en 138h Sv.

Artikel 138g Sv luidt:

“Onder aanbieder van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.”

Artikel 138h Sv luidt:

“Onder gebruiker van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst.”

5.1.3 In aanvulling op de bevoegdheden van artikel 126n en 126na Sv voorziet artikel 126ng Sv in een regeling om een vordering tot het verstrekken van gegevens te richten tot een aanbieder van een communicatiedienst. Het gaat dan om gevallen waarin de vordering betrekking heeft op andere gegevens dan de gegevens zoals bedoeld in artikel 126n en 126na Sv. Artikel 126ng Sv maakt het, kort gezegd, mogelijk dat dan de bevoegdheden tot het vorderen van gegevens, zoals geregeld in artikel 126nc (identificerende gegevens), 126nd (andere dan identificerende gegevens) en 126ne (toekomstige gegevens) Sv, worden toegepast. Daarbij stelt artikel 126ng lid 2 Sv aanvullende eisen als de vordering betrekking heeft op gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn.

Artikel 126ng Sv luidt:

> "1. Een vordering als bedoeld in artikel 126nc, eerste lid, 126nd, eerste lid, of 126ne, eerste en derde lid, en artikel 126nf, eerste lid kan worden gericht tot de aanbieder van een communicatiedienst in de zin van artikel 138g, voor zover de vordering betrekking heeft op andere gegevens dan die welke gevorderd kunnen worden door toepassing van de artikelen 126n en 126na. De vordering kan geen betrekking hebben op gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn.
>
> 2. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van de aanbieder van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot gegevens als bedoeld in de laatste volzin van het eerste lid, deze gegevens vorderen, voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend, of klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd.
>
> 3. Een vordering als bedoeld in het tweede lid kan niet worden gericht tot de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.
>
> 4. Een vordering als bedoeld in het tweede lid kan slechts worden gedaan na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 1261, zevende lid, is van overeenkomstige toepassing.
>
> 5. Artikel 126nd, derde tot en met vijfde en zevende lid, is van overeenkomstige toepassing."

5.1.4 Daarnaast voorziet artikel 126ni lid 1 Sv in de bevoegdheid om van degene van wie redelijkerwijs wordt vermoed dat hij toegang heeft tot bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk en waarvan redelijkerwijs kan worden aangenomen dat zij in het bijzonder vatbaar zijn voor verlies of wijziging, vorderen dat deze gegevens voor een periode van ten hoogste negentig dagen worden bewaard en beschikbaar gehouden. Het tweede lid van artikel 126ni Sv bepaalt dat indien deze vordering wordt gericht tot een aanbieder van een communicatiedienst en de vordering betrekking heeft of mede betrekking heeft op gegevens als bedoeld in artikel 126n lid 1 Sv (dus gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker), de aanbieder verplicht is zo spoedig mogelijk de gegevens te verschaffen die nodig zijn om de identiteit te achterhalen van andere aanbieders van wier dienst bij de communicatie gebruik is gemaakt. Aan de bevoegdheid van artikel 126ni Sv kan toepassing worden gegeven in geval van verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane strafbare feiten een ernstige inbreuk op de rechtsorde oplevert.

Artikel 126ni Sv luidt:

> “1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk en waarvan redelijkerwijs kan worden aangenomen dat zij in het bijzonder vatbaar zijn voor verlies of wijziging, vorderen dat deze gegevens gedurende een periode van ten hoogste negentig dagen worden bewaard en beschikbaar gehouden. De vordering kan niet worden gericht tot de verdachte.
>
> 2. Indien de vordering is gericht tot de aanbieder van een communicatiedienst in de zin van artikel 138g en de vordering betrekking of mede betrekking heeft op gegevens als bedoeld in artikel 126n, eerste lid, is de aanbieder verplicht zo spoedig mogelijk de gegevens te verschaffen die nodig zijn om de identiteit te achterhalen van andere aanbieders van wier dienst bij de communicatie gebruik is gemaakt.
>
> 3. De vordering wordt schriftelijk of mondeling gedaan. Indien de vordering mondeling wordt gedaan, doet de officier van justitie de vordering zo spoedig mogelijk op schrift stellen en doet hij binnen drie dagen nadat de vordering mondeling is gedaan, een gewaarmerkt afschrift daarvan verstrekken aan degene tot wie de vordering is

gericht. Bij de vordering en bij het op schrift stellen daarvan worden vermeld:

a. een zo nauwkeurig mogelijke omschrijving van de gegevens die beschikbaar moeten worden gehouden;

b. het tijdstip van de vordering;

c. de titel van de vordering;

d. de periode gedurende de welke de gegevens beschikbaar moeten blijven, en

e. of het tweede lid van toepassing is.

4. De officier van justitie doet van de vordering en, indien deze mondeling plaatsvond, van de schriftelijke vastlegging daarvan een proces-verbaal opmaken, waarin worden vermeld:

a. de gegevens, bedoeld in het derde lid;

b. het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte; en

c. de feiten of omstandigheden waaruit blijkt dat is voldaan aan de voorwaarden, bedoeld in het eerste lid.

5. De vordering kan ten hoogste eenmaal worden verlengd voor een periode van ten hoogste negentig dagen. Het tweede, derde en vierde lid zijn van overeenkomstige toepassing."

5.2 De onder 5.1 besproken bevoegdheden kunnen ook worden toegepast als uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren (vgl. artikel 126o lid 1 Sv), en tevens in geval van aanwijzingen van een terroristisch misdrijf. Dit is geregeld in artikel 126u, 126ua, 126ug, 126ui, 126zh, 126zi, 126zja en 126zo Sv.

Artikel 126u Sv luidt:

"1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst in de zin van artikel 1261a en het communicatieverkeer met betrekking tot die gebruiker. De vordering

kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:

a. ten tijde van de vordering zijn verwerkt, dan wel

b. na het tijdstip van de vordering worden verwerkt.

2. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een communicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing. Indien de vordering, bedoeld in het eerste lid, betrekking heeft op een persoon die aanspraak kan maken op bronbescherming, kan deze slechts worden gedaan na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 218a, tweede lid, is van overeenkomstige toepassing.

3. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering gedaan voor een periode van ten hoogste drie maanden.

4. De officier van justitie doet van de vordering proces-verbaal opmaken, waarin worden vermeld:

a. een omschrijving van het georganiseerd verband;

b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;

c. indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon omtrent wie gegevens worden gevorderd;

d. de gegevens die worden gevorderd;

e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, de periode waarover de vordering zich uitstrekt.

5. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in het eerste lid, eerste volzin. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering doet de officier van justitie proces-verbaal opmaken.

6. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de officier van justitie worden gevorderd.”

Artikel 126ua Sv luidt:

"1. In een geval als bedoeld in artikel 126o, eerste lid, kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst in de zin van artikel 1261a. Artikel 126u, tweede lid, is van toepassing.

2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126t of artikel 126u, kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt.

3. In geval van een vordering als bedoeld in het eerste of tweede lid is artikel 126u, vierde lid, onder a, b, c en d, van overeenkomstige toepassing en blijft artikel 126bb buiten toepassing.

4. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de opsporingsambtenaar of de officier van justitie worden gevorderd."

Artikel 126ug Sv luidt:

"1. Een vordering als bedoeld in artikel 126uc, eerste lid, 126ud, eerste lid, of 126ue, eerste en derde lid, en artikel 126uf, eerste lid kan worden gericht tot de aanbieder van een openbaar of een niet-openbaar telecommunicatienetwerk, onderscheidenlijk de aanbieder van een openbare of een niet-openbare telecommunicatiedienst, voor zover de vordering betrekking heeft op andere gegevens dan die welke gevorderd kunnen worden door toepassing van de artikelen 126u en 126ua. De vordering kan geen betrekking hebben op gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn.

2. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van de aanbieder van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot gegevens als bedoeld in de laatste volzin van het eerste lid, deze gegevens vorderen, voor zover zij klaarblijkelijk afkomstig zijn van een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven, voor hem bestemd zijn, op hem betrekking hebben of hebben gediend tot het in dat georganiseerd verband beramen of plegen van een misdrijf, of klaarblijkelijk met betrekking tot die

gegevens in dat georganiseerd verband een misdrijf wordt beraamd of gepleegd.

3. Een vordering als bedoeld in het tweede lid kan niet worden gericht tot de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.

4. Een vordering als bedoeld in het tweede lid kan slechts worden gedaan na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 1261, zevende lid, is van overeenkomstige toepassing.

5. Artikel 126nd, derde tot en met vijfde en zevende lid, is van overeenkomstige toepassing."

Artikel 126ui Sv luidt:

"1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk en waarvan redelijkerwijs kan worden aangenomen dat zij in het bijzonder vatbaar zijn voor verlies of wijziging, vorderen dat deze gegevens gedurende een periode van ten hoogste negentig dagen worden bewaard en beschikbaar gehouden. De vordering kan niet worden gericht tot de verdachte.

2. Artikel 126ni, tweede tot en met vijfde lid, is van overeenkomstige toepassing, met dien verstande dat bij de in artikel 126ni, vierde lid, onderdeel c, bedoelde feiten en omstandigheden ook een omschrijving van het in artikel 126o, eerste lid, bedoelde georganiseerde verband wordt opgenomen."

Artikel 126zh Sv luidt:

"1. In geval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst in de zin van artikel 1261a en het communicatieverkeer met betrekking tot die gebruiker. De vordering kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:

a. ten tijde van de vordering zijn verwerkt, dan wel

b. na het tijdstip van de vordering worden verwerkt.

2. Artikel 126n, tweede tot en met zesde lid, is van overeenkomstige toepassing.”

Artikel 126zi Sv luidt:

“1. In geval van aanwijzingen van een terroristisch misdrijf kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst in de zin van artikel 138h. Artikel 126n, tweede lid, is van toepassing.

2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126zf of artikel 126zg kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt.

3. Artikel 126na, derde en vierde lid, is van overeenkomstige toepassing.”

Artikel 126zja Sv luidt:

“1. In geval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk en waarvan redelijkerwijs kan worden aangenomen dat zij in het bijzonder vatbaar zijn voor verlies of wijziging, vorderen dat deze gegevens gedurende een periode van ten hoogste negentig dagen worden bewaard en beschikbaar gehouden. De vordering kan niet worden gericht tot de verdachte.

2. Artikel 126ni, tweede tot en met vijfde lid, is van overeenkomstige toepassing.”

Artikel 126zo Sv luidt:

“1. Een vordering als bedoeld in artikel 126zk, eerste lid, 126zl, eerste lid, of 126zm, eerste lid, kan worden gericht tot de aanbieder van een communicatiedienst in de zin van artikel 138g, voor zover de vordering betrekking heeft op andere gegevens dan die welke gevorderd kunnen worden door toepassing van de artikelen 126zh en 126zi. De vordering kan geen betrekking hebben op gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn.

2. Indien het belang van het onderzoek dit dringend vordert, kan de officier van justitie van de aanbieder van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot gegevens als bedoeld in het eerste lid, laatste volzin, deze gegevens vorderen.

3. Artikel 126nd, derde tot en met vijfde en zevende lid, en 126nf, tweede en derde lid, zijn van overeenkomstige toepassing."

5.3 De algemene maatregel van bestuur waarnaar in artikel 126n, 126u en 126zh Sv wordt verwezen, betreft het Besluit vorderen gegevens telecommunicatie. Dit besluit houdt onder meer in:

"Artikel 1

In dit besluit wordt verstaan onder:

a. gebruiker: een gebruiker als bedoeld in artikel 138h van het Wetboek van Strafvordering;

b. nummer: een nummer als bedoeld in artikel 1.1 van de Telecommunicatiewet.

Artikel 2

De volgende gegevens worden aangewezen als gegevens in de zin van artikel 126n, eerste lid, tweede volzin, artikel 126u, eerste lid, tweede volzin, en artikel 126zh, eerste lid, tweede volzin, van het Wetboek van Strafvordering:

a. de naam, het adres en de woonplaats van de gebruiker;

b. de nummers van de gebruiker;

c. de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen;

d. de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, ingeval er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen, alsmede de afwijking van dit tijdstip van de wettelijke tijd, bedoeld in artikel 1, eerste lid, van de wet van 16 juli 1958 tot nadere regeling van de wettelijke tijd (Stb. 352);

e. de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe;

f. de nummers van de randapparatuur waarvan de gebruiker gebruik maakt of heeft gemaakt;

g. de soorten diensten waarvan de gebruiker gebruik maakt of heeft gemaakt evenals de daarbij behorende gegevens;

h. de naam, het adres en de woonplaats van degene die de rekening betaalt voor de openbare telecommunicatiediensten en telecommunicatienetwerken die de gebruiker ter beschikking heeft of heeft gehad, indien deze een ander is dan de gebruiker.

5.4.1 Van het doen van een vordering om de onder 5.1 genoemde gegevens te verstrekken wordt proces-verbaal opgemaakt.[3] Deze processen-verbaal en overige stukken die verband houden met de uitoefening van deze bevoegdheden worden, voor zover die van betekenis zijn voor het onderzoek in de zaak, bij de processtukken gevoegd zodra het belang van het onderzoek dat toelaat.[4] Ook als geen proces-verbaal is opgemaakt, wordt van de uitoefening van de bevoegdheden melding gemaakt in de processtukken.[5] De verdachte kan van deze processtukken kennisnemen. Dat is alleen anders als op grond van artikel 149b Sv vanwege - kort gezegd - zwaarwegende redenen voeging bij de processtukken achterwege blijft.[6]

5.4.2 Artikel 126bb Sv voorziet daarnaast in een zogenoemde notificatieverplichting. Op grond van artikel 126bb lid 1 Sv doet de officier van justitie aan de betrokkene schriftelijk mededeling van de uitoefening van onder meer de bevoegdheden die zijn neergelegd in artikel 126n, 126ng, 126ni, 126u, 126ug, 126ui,126zh, 126zja en 126zo Sv, zodra het belang van het onderzoek dat toelaat. Deze verplichting vormt een aanvulling op de regeling van de kennisneming van de processtukken, en strekt ertoe dat ook anderen dan de verdachte op de hoogte komen van de uitoefening van de betreffende bevoegdheden. De notificatieverplichting ziet niet op de uitoefening van de bevoegdheden die zijn neergelegd in artikel 126na, 126ua en 126zi Sv.

3 Artikel 126n lid 4, 126na lid 3, 126ng lid 5 in verbinding met 126nd lid 5, 126ni lid 4, 126u lid 4, 126ua lid 3, 126ug lid 5 in verbinding met 126nd lid 5, 126ui lid 2 in verbinding met 126ni lid 4, 126zh lid 2, 126zh lid 3, 126zja lid 2 in verbinding met 126ni lid 4, en 126zo lid 3 in verbinding met 126nd lid 5 Sv.

4 Artikel 126aa lid 1 Sv en artikel 149a lid 2 Sv.

5 Artikel 126aa lid 4 Sv.

6 Zie naast artikel 149b Sv (in verbinding met artikel 187d lid 1 Sv) ook artikel 126aa lid 4, tweede volzin, Sv.

5.4.3 Artikel 126cc lid 1 Sv schrijft voor, voor zover hier van belang, dat zolang de zaak niet is geëindigd, de officier van justitie de processen-verbaal en andere voorwerpen bewaart waaraan gegevens kunnen worden ontleend die zijn verkregen door het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, voor zover de betreffende stukken niet bij de processtukken zijn gevoegd. De officier van justitie houdt deze processen-verbaal en andere voorwerpen ter beschikking van het onderzoek. Na afloop van de zaak gaat de officier van justitie over tot vernietiging daarvan, overeenkomstig artikel 126cc leden 2 en 3 Sv. De wijze van bewaring en vernietiging is nader geregeld in het Besluit bewaren en vernietigen niet-gevoegde stukken. Van vernietiging kan worden afgezien, zo bepaalt artikel 126dd lid 1 Sv, als de betreffende gegevens kunnen worden gebruikt voor een ander strafrechtelijk onderzoek dan waartoe de bevoegdheid is uitgeoefend, of in bepaalde gevallen voor de verwerking op grond van de Wet politiegegevens. In die gevallen regelt het tweede lid van artikel 126dd Sv wanneer de gegevens alsnog worden vernietigd.

5.5 Het Wetboek van Strafvordering voorziet niet in een algemene verplichting voor telecommunicatieaanbieders om de gegevens vast te leggen die met toepassing van de hiervoor besproken bevoegdheden kunnen worden gevorderd.[7] Zoals in de vordering van de advocaat-generaal onder 20-22 nader is uiteengezet, zijn de bepalingen die - met het oog op criminaliteitsbestrijding - in de Telecommunicatiewet zijn opgenomen en die betrekking hebben op bewaartermijnen voor verkeers- en locatiegegevens alsmede voor identificerende gegevens, door de rechter buiten werking gesteld. Die buitenwerkingstelling was het gevolg van het ongeldig verklaren van de zogenoemde Dataretentie-richtlijn door het Hof van Justitie.[8] De wetgeving die beoogt te voorzien in een gewijzigde regeling van deze bewaarplichten, is nog in voorbereiding.[9] Het Wetboek van Strafvordering voorziet wel in de uitoefening van de hiervoor besproken bevoegdheden ten aanzien van gegevens die op een andere grond dan deze buiten werking gestelde wettelijke bepalingen zijn vastgelegd en bewaard.

Unierecht

5.6 Het Unierecht stelt regels met betrekking tot het verwerken en het bewaren van verkeers- en locatiegegevens (daaronder begrepen ook identificerende

7 Specifieke bewaarplichten voor zover die voortvloeien uit de regelingen van artikel 126ni en artikel 126n lid 1, aanhef en onder b, Sv, komen aan de orde in rechtsoverwegingen 6.3.3-6.3.4.

8 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.

9 Wetsvoorstel 34537.

gegevens[10]) door aanbieders van elektronische-communicatiediensten. Deze regels zijn neergelegd in Richtlijn 2002/58/EG. De van belang zijnde bepalingen van deze richtlijn luiden als volgt:

> "Artikel 1
>
> Werkingssfeer en doelstelling
>
> 1. Deze richtlijn harmoniseert de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming 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 en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronische-communicatieapparatuur en -diensten in de Gemeenschap.
>
> 2. Voor op de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op Richtlijn 95/46/EG. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn.
>
> 3. Deze richtlijn is niet van toepassing op (...) de activiteiten van de staat op strafrechtelijk gebied.
>
> Artikel 2
>
> Definities
>
> Tenzij anders is bepaald, zijn de definities van Richtlijn 95/46/EG van het Europees Parlement en de Raad en Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (kaderrichtlijn) van toepassing.
>
> Daarnaast wordt in deze richtlijn verstaan onder:
>
> a) "gebruiker": natuurlijke persoon die gebruikmaakt van een openbare elektronische- communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

[10] Onder 'verkeersgegevens' worden verstaan: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch-communicatienetwerk of voor de facturering daarvan (artikel 2, onder b, Richtlijn 2002/58/EG). Daaronder vallen naamgevings-, nummerings- of adresseringsgegevens die door de verzender van een communicatie of door de gebruiker van een verbinding worden verstrekt om de communicatie tot stand te brengen. Wanneer deze gegevens door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren deze ook tot de verkeersgegevens. Zie de preambule bij Richtlijn 2002/58/EG, onder 15.

b) “verkeersgegevens”: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan;

c) “locatiegegevens”: gegevens die in een elektronische-communicatienetwerk of door een elektronische-communicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronische-communicatiedienst wordt aangegeven;

d) “communicatie”: informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische-communicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

(...)

Artikel 3

Betrokken diensten

Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.

(...)

Artikel 5

Vertrouwelijk karakter van de communicatie

1. De lidstaten garanderen 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 de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.

2. Lid 1 laat de bij de wet toegestane registratie van communicatie en de daarmee verband houdende verkeersgegevens onverlet, wanneer die wordt uitgevoerd in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van enigerlei andere zakelijke communicatie.

3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.

Artikel 6

Verkeersgegevens

1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.

2. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.

3. De aanbieder van een openbare elektronische-communicatiedienst mag ten behoeve van de marketing van elektronische-communicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

(...)

Artikel 9

Andere locatiegegevens dan verkeersgegevens

1. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voorzover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden.

HvJ EU 2 oktober 2018, zaak C-207/16, ECLI:EU:C:2018:788 (Ministerio Fiscal). Bij verwijzingen naar het hier genoemde arrest wordt de aanduiding Ministerio Fiscal gebruikt.

HvJ EU 2 maart 2021, zaak C-746/18, ECLI:EU:C:2021:152 (H.K., in tegenwoordigheid van Prokuratuur). Bij verwijzingen naar het hier genoemde arrest wordt de aanduiding Prokuratuur gebruikt.

HvJ EU 21 december 2016, zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (Tele2 Sverige AB tegen Post- och telestyrelsen, en Secretary of State for the Home Department [redacted]

e.a.); HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (La Quadrature du Net e.a. tegen Premier ministre e.a.). Bij verwijzingen naar de hier genoemde arresten worden deze respectievelijk aangeduid als Tele2 en Quadrature.

(...)

Artikel 15

Toepassing van een aantal bepalingen van Richtlijn 95/46/EG

1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1,2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is 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 als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie."

5.7 Het Hof van Justitie is in de zaken Tele2 Sverige en [redacted] en La Quadrature du Net e.a. ingegaan op, kort gezegd, de vraag onder welke voorwaarden een verplichting voor aanbieders van elektronische-communicatiediensten om verkeers- en locatiegegevens te bewaren met het oog op - kort gezegd - de bestrijding van criminaliteit verenigbaar is met artikel 15 lid 1 Richtlijn 2002/58/EG.[11] In deze rechtspraak en in de zaak Ministerio Fiscal[12] is het Hof van Justitie (tevens) ingegaan op de vraag onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang kan worden verleend tot gegevens die zijn bewaard door de aanbieders van elektronische-communicatiediensten. De van belang zijnde overwegingen uit de arresten van het Hof van Justitie zijn weergegeven in de vordering van de advocaat-generaal onder 26-41.

11 HvJ EU 21 december 2016, zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (Tele2 Sverige AB tegen Postoch telestyrelsen, en Secretary of State for the Home Department [redacted] e.a.); HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (La Quadrature du Net e.a. tegen Premier ministre e.a.). Bij verwijzingen naar de hier genoemde arresten worden deze respectievelijk aangeduid als Tele2 en Quadrature.

12 HvJ EU 2 oktober 2018, zaak C-207/16, ECLI:EU:C:2018:788 (Ministerio Fiscal). Bij verwijzingen naar het hier genoemde arrest wordt de aanduiding Ministerio Fiscal gebruikt.

5.8 In de zaak Prokuratuur heeft het Hof van Justitie prejudiciële vragen beantwoord die betrekking hebben op de voorwaarden waaronder het verlenen van toegang aan overheidsinstanties tot een reeks verkeers- en locatiegegevens kan worden toegestaan.[13] Daarnaast is het Hof van Justitie ingegaan op de vereisten met betrekking tot de (rechterlijke) toetsing voorafgaand aan het verlenen van toegang tot bewaarde gegevens en, in verband daarmee, de vraag of deze toetsing ook mag plaatsvinden door de openbaar aanklager. De van belang zijnde overwegingen uit dit arrest zijn weergegeven in de vordering van de advocaat-generaal onder 42-47.

5.9 De Hoge Raad gaat hierna nader in op de betekenis en de (mogelijke) gevolgen van deze rechtspraak van het Hof van Justitie voor de toepassing van de onder 5.1 en 5.2 genoemde bevoegdheden in het Wetboek van Strafvordering.

6. Betekenis en (mogelijke) gevolgen van het Unierecht voor de toepassing van de bevoegdheden in het Wetboek van Strafvordering

6.1 De rechtspraak van het Hof van Justitie over het bewaren en het verlenen van toegang tot in het bijzonder verkeers- en locatiegegevens heeft - zoals naar voren komt in de vordering van de advocaat-generaal - in de rechtspraktijk aanleiding gegeven tot vragen over de verhouding tussen enerzijds de onder 5.1 en 5.2 besproken bevoegdheden in het Wetboek van Strafvordering en anderzijds het Unierecht. In het navolgende gaat de Hoge Raad in op verschillende van deze vragen.

Toepassingsbereik van Richtlijn 2002/58/EG en de rechtspraak van het Hof van Justitie over die richtlijn

6.2.1 Richtlijn 2002/58/EG heeft blijkens artikel 1 lid 1 betrekking op “de verwerking van persoonsgegevens in de sector elektronische communicatie”. Deze richtlijn is van toepassing in gevallen waarin een lidstaat maatregelen treft met betrekking tot het verwerken van dergelijke gegevens door aanbieders van elektronische-communicatiediensten en het verlenen van toegang van overheidsinstanties tot die gegevens. Richtlijn 2002/58/EG is daarmee van belang voor de toepassing van de onder 5.1 en 5.2 besproken wettelijke bevoegdheden. Maatregelen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie zonder dat daarbij verwerkingsverplichtingen worden opgelegd aan aanbieders van elektronische-communicatiediensten, vallen echter buiten het bereik van

[13] HvJ EU 2 maart 2021, zaak C-746/18, ECLI:EU:C:2021:152 (H.K., in tegenwoordigheid van Prokuratuur). Bij verwijzingen naar het hier genoemde arrest wordt de aanduiding Prokuratuur gebruikt.

Richtlijn 2002/58/EG.[14] De Hoge Raad leidt daaruit af dat bijvoorbeeld het onderzoek aan inbeslaggenomen telefoontoestellen buiten het toepassingsbereik van Richtlijn 2002/58/EG valt.

6.2.2 In de onder 5.7 en 5.8 genoemde rechtspraak van het Hof van Justitie staat bij de beoordeling van de mogelijkheid om verkeers- en locatiegegevens te bewaren en te (doen) verstrekken de betekenis centraal van artikel 15 lid 1 Richtlijn 2002/58/EG alsmede van de in het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest) neergelegde rechten op eerbiediging van het privéleven, bescherming van persoonsgegevens en vrijheid van meningsuiting en van informatie.[15] Artikel 15 lid 1 Richtlijn 2002/58/EG heeft daarbij mede betrekking op de wettelijke maatregelen die de lidstaten kunnen treffen om gegevens gedurende een beperkte periode te bewaren in verband met onder meer het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

6.2.3 Het Wetboek van Strafvordering kent, voor zover hier van belang, alleen bevoegdheden tot het vorderen van verkeers- en locatiegegevens alsmede identificerende gegevens. Er geldt, als gevolg van de onder 5.5 besproken buitenwerkingstelling door de rechter van een aantal bepalingen van de Telecommunicatiewet, geen algemene wettelijke bewaarplicht met betrekking tot die gegevens. Voorwerp van toepassing van de in het Wetboek van Strafvordering neergelegde bevoegdheden zijn daarom gegevens die op een andere (bijvoorbeeld contractuele) grond worden bewaard door aanbieders van een communicatiedienst.

Gelet op deze buitenwerkingstelling door de rechter van een aantal bepalingen van de Telecommunicatiewet, is het voor de Nederlandse situatie van belang te weten of de overwegingen van het Hof van Justitie in de onder 5.7 en 5.8 genoemde rechtspraak, voor zover het daarin gaat om de toegang tot verkeers- en locatiegegevens (met inbegrip van identificerende gegevens), betrekking hebben op alleen gegevens die worden bewaard op grond van wettelijke maatregelen die door een lidstaat op grond van

[14] Quadrature, overweging 103: “Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronischecommunicatiediensten, wordt de bescherming van de gegevens van de betrokken personen niet beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende 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, en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (PB 2016, L 119, blz. 89), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM.”

[15] Artikelen 7, 8 en 11 Handvest.

artikel 15 lid 1 Richtlijn 2002/58/EG zijn getroffen, dan wel ook op gegevens die op een andere, bijvoorbeeld contractuele, grond worden bewaard.

6.2.4 Naar het oordeel van de Hoge Raad moet deze vraag, om de hierna genoemde redenen, aldus worden beantwoord dat de overwegingen van het Hof van Justitie in de onder 5.7 en 5.8 genoemde rechtspraak tevens betrekking hebben op het in het kader van een strafrechtelijk onderzoek verlenen van toegang tot de onder 6.2.3 genoemde gegevens, die op een andere grond worden bewaard dan wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG.

Allereerst is van belang dat Richtlijn 2002/58/EG beoogt de bescherming 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.[16] Die doelstelling is van belang ongeacht of het gaat om gegevens die worden bewaard op grond van wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG of om gegevens die worden bewaard op een andere grond.

Artikel 5 Richtlijn 2002/58/EG strekt verder ertoe dat niet slechts het afluisteren, aftappen of opslaan maar ook het "anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers" alleen is geoorloofd als dat bij wet is toegestaan overeenkomstig artikel 15 lid 1 Richtlijn 2002/58/EG. Dat duidt erop dat de wettelijke maatregelen waarop artikel 15 lid 1 Richtlijn 2002/58/EG ziet, niet alleen betrekking (kunnen) hebben op het bewaren van verkeersgegevens, maar ook op het verkrijgen van toegang tot die gegevens. Dat brengt dan met zich dat de regeling in het Wetboek van Strafvordering van de bevoegdheden die ertoe strekken dat ten behoeve van de opsporing en vervolging van strafbare feiten verkeersgegevens kunnen worden verkregen, moet worden opgevat als een wettelijke maatregel in de zin van artikel 15 lid 1 Richtlijn 2002/58/EG. Uit het samenstel van artikel 9 en 15 lid 1 Richtlijn 2002/58/EG moet worden afgeleid dat een en ander ook geldt in relatie tot locatiegegevens.[17]

16 Zie artikel 1 lid 1 Richtlijn 2002/58/EG.

17 Zie ook Tele2, overweging 78, waarin wordt overwogen dat onder de werkingssfeer van Richtlijn 2002/58/EG valt "een wettelijke maatregel waarbij een lidstaat op grond van artikel 15, lid 1, van richtlijn 2002/58, ter verwezenlijking van de in die bepaling vermelde doelstellingen, aan de aanbieders van elektronischecommunicatiediensten de verplichting oplegt om de nationale autoriteiten onder de in een dergelijke maatregel genoemde voorwaarden toegang te verlenen tot de door die aanbieders bewaarde gegevens". In latere rechtspraak is deze overweging herhaald, zij het in enigszins andere bewoordingen, die mogelijk tegenstrijdig zijn met de zojuist geciteerde formulering. Zie Ministerio Fiscal, overweging 35 en Quadrature, overweging 96, en in verband daarmee de vordering van de advocaat-generaal onder 60.

Hiernaast duiden de bewoordingen van de arresten van het Hof van Justitie erop dat de beantwoording van de vraag onder welke voorwaarden de toegang tot bewaarde verkeers- en locatiegegevens kan worden toegestaan, niet afhankelijk is van "de omvang van de aan de aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot bewaring van gegevens".[18] In deze rechtspraak worden die voorwaarden niet uitsluitend in verband gebracht met gegevens die worden bewaard op grond van wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG.[19] Het gaat tevens om gegevens die door een aanbieder zijn bewaard in overeenstemming met artikel 5, 6 en 9 Richtlijn 2002/58/EG.[20]

6.2.5 Gelet op het vorenstaande neemt de Hoge Raad tot uitgangspunt dat de rechtspraak van het Hof van Justitie, voor zover het daarin gaat om het verlenen van toegang tot verkeers- en locatiegegevens (met inbegrip van identificerende gegevens), betrekking heeft op niet alleen gegevens die worden bewaard op grond van wettelijke maatregelen die door een lidstaat zijn getroffen op grond van artikel 15 lid 1 Richtlijn 2002/58/EG, maar tevens op de onder 6.2.3 genoemde gegevens, die op een andere grond worden bewaard dan wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG. De Hoge Raad vindt echter aanleiding tot het stellen van een prejudiciële vraag aan het Hof van Justitie. De reden daarvoor is dat de rechtspraak van het Hof van Justitie geen expliciet antwoord bevat op de onder 6.2.3 genoemde vraag, terwijl - zoals volgt uit de vordering van de advocaat-generaal onder 61 - aan het Unierecht ook argumenten kunnen worden ontleend voor een andersluidende beantwoording dan onder 6.2.4 is weergegeven.

Voorwaarden met betrekking tot het verlenen van toegang aan overheidsinstanties

6.3.1 Het Hof van Justitie heeft in de onder 5.7 en 5.8 genoemde rechtspraak onder meer de voorwaarden uitgewerkt die gelden met betrekking tot (i) het bewaren van verkeers- en locatiegegevens en (ii) het verlenen van toegang aan overheidsinstanties tot bewaarde verkeers- en locatiegegevens. Het Hof van Justitie heeft bij het ontwikkelen van die voorwaarden in het bijzonder in aanmerking genomen onder welke omstandigheden en met inachtneming van welke waarborgen het bewaren van verkeers- en locatiegegevens en het verlenen van toegang tot die gegevens, mede gelet op het evenredigheidsbeginsel, verenigbaar is met de in het Handvest neergelegde

18 Tele2, overweging 113.

19 Vgl. Tele2, overweging 125; Prokuratuur, overweging 45.

20 Quadrature, overweging 167.

rechten op eerbiediging van het privéleven, bescherming va persoonsgegevens en vrijheid van meningsuiting en van informatie.[21]

6.3.2 Gelet op wat onder 5.5 is overwogen over het ontbreken van een algemene wettelijke bewaarplicht kent het Nederlandse recht, met uitzondering van wat hierna onder 6.3.3 en 6.3.4 aan de orde komt, geen wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG. Het onder 6.2.5 geformuleerde uitgangspunt brengt echter met zich dat als toepassing wordt gegeven aan de onder 5.1 en 5.2 besproken bevoegdheden uit het Wetboek van Strafvordering, wel moet worden voldaan aan de voorwaarden die door het Hof van Justitie zijn geformuleerd voor het verlenen van toegang aan overheidsinstanties tot bewaarde verkeers- en locatiegegevens.

6.3.3 Dat er naar Nederlands recht geen algemene wettelijke bewaarplicht geldt, neemt niet weg dat er wel specifieke en beperkte bewaarplichten kunnen worden aangewezen. Zo maakt de regeling van artikel 126ni Sv (zie ook artikel 126ui en 126zja Sv) het onder omstandigheden mogelijk dat een vordering wordt gericht tot een aanbieder van een communicatiedienst die ertoe strekt dat bepaalde gegevens van een gebruiker worden bewaard en beschikbaar gehouden voor een periode van 90 dagen. Daarbuiten kan een vordering tot het verstrekken van verkeers- en locatiegegevens zich ook uitstrekken tot gegevens die "na het tijdstip van de vordering worden verwerkt" (artikel 126n lid 1, aanhef en onder b, Sv; zie ook artikel 126u lid 1 en 126zh lid 1 Sv). Het gaat dan om het verstrekken van zogenoemde toekomstige gegevens die door de aanbieder van de communicatiedienst in het kader van zijn bedrijfsactiviteiten worden verwerkt na het tijdstip van de vordering. Daarmee strekt deze bevoegdheid ertoe dat die verwerkte gegevens niet verloren gaan en ook niet worden gewijzigd, maar dat deze worden vastgelegd en ongewijzigd aan de officier van justitie worden verstrekt.

In dit verband kan worden gewezen op de overwegingen van het Hof van Justitie in de zaak La Quadrature du Net e.a. over de zogenoemde spoedbewaring:

"160 Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die richtlijn moeten worden verwerkt en opgeslagen.

[21] Artikelen 7, 8 en 11 Handvest.

161 Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162 In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen - nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

163 In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164 Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die

een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165 In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet- discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voorde nationale veiligheid, is voorbereid of gepleegd. Bovendien moet aan de bevoegde autoriteiten toegang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin richtlijn 2002/58 is uitgelegd (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 118-121 en aldaar aangehaalde rechtspraak).

166 Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van

bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mits de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167 In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58."

6.3.4 De hiervoor geciteerde overwegingen hebben in de kern betrekking op de spoedbewaring van gegevens die door de aanbieder van de elektronische-communicatiedienst al bewaard werden, maar die zonder zo'n spoedbewaring mogelijk verloren zouden gaan, waardoor ook geen mogelijkheid meer zou bestaan om toegang tot die gegevens te verlenen. Zo'n bevoegdheid tot het vorderen van spoedbewaring is neergelegd in artikel 126ni Sv. De geciteerde overwegingen lijken daarnaast betekenis te hebben voor de bevoegdheid om de verstrekking van toekomstige verkeers- en locatiegegevens te vorderen, in gevallen waarin het niet zeker is dat de betreffende gegevens in het kader van de normale bedrijfsuitoefening van de aanbieder van de communicatiedienst bewaard zouden blijven. Dat brengt met zich dat bij de toepassing van de bevoegdheid om de verstrekking van die toekomstige gegevens te vorderen, mede acht moet worden geslagen op de voorwaarden die het Hof van Justitie stelt aan spoedbewaring en aan het verlenen van toegang tot aldus bewaarde gegevens.

6.4.1 Waar het gaat om de voorwaarden voor het verlenen van toegang aan overheidsinstanties tot gegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, houdt de uitspraak van het Hof van Justitie in de zaak Tele2 Sverige en [redacted] onder meer het volgende in:

"115 Met betrekking tot de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling die een uitzondering maakt op het beginsel van de vertrouwelijkheid van de elektronische communicatie, dient eraan te worden herinnerd dat, aangezien de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gegeven opsomming van de doelstellingen exhaustief is, zoals in de punten 90 en 102 van het onderhavige arrest is vastgesteld, de toegang tot de bewaarde gegevens daadwerkelijk en strikt op een van die doelstellingen moet berusten. Daarbij komt dat, aangezien het met deze

regeling nagestreefde doel in verhouding moet staan tot de ernst van de ingreep in de grondrechten die deze toegang meebrengt, ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten alleen de bestrijding van zware criminaliteit een dergelijke toegang tot de bewaarde gegevens kan rechtvaardigen.

116 Wat de eerbiediging van het evenredigheidsbeginsel betreft, moet een nationale regeling betreffende de voorwaarden waaronder de aanbieders van elektronischecommunicatiediensten aan de bevoegde nationale autoriteiten toegang tot de bewaarde gegevens moeten verlenen, waarborgen dat, overeenkomstig hetgeen in de punten 95 en 96 van het onderhavige arrest is vastgesteld, een dergelijke toegang niet verdergaat dan strikt noodzakelijk is.

(...)

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 nationale 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 ofte hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf (zie naar analogie EHRM, 4 december 2015, [redacted] 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 de bestrijding van dergelijke activiteiten zouden kunnen leveren.

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 (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest Digital Rights, punt 62; zie ook naar analogie, met betrekking tot

artikel 8 EVRM, EHRM, 12januari 2016, Szabó en Vissy tegen Hongarije, CE:ECHR:2016:0112JUD003713814, §§ 77 en 80).

121 Verder is het van belang dat de bevoegde nationale autoriteiten waaraan toegang tot de bewaarde gegevens is verleend, in het kader van de toepasselijke nationale procedures de betrokken personen daarvan op de hoogte brengen wanneer zulks de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen. Dit is immers noodzakelijk om de betrokken personen in staat te stellen om, in geval van schending van hun rechten, met name gebruik te maken van het recht van beroep, waarin artikel 15, lid 2, van richtlijn 2002/58, gelezen in samenhang met artikel 22 van richtlijn 95/46, uitdrukkelijk voorziet (zie naar analogie arresten van 7 mei 2009, [redacted] C-553/07, EU:C:2009:293, punt 52, en 6 oktober 2015, Schrems, C- 362/14, EU:C:2015:650, punt 95).

(...)

124 Het staat aan de verwijzende rechterlijke instanties, na te gaan of en in welke mate de in het hoofdgeding aan de orde zijnde nationale regelingen, zowel ter zake van de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens als ter zake van de bescherming en het niveau van beveiliging van deze gegevens, voldoen aan de eisen die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zoals die in de punten 115 tot en met 123 van het onderhavige arrest nader zijn uiteengezet.

125 Gelet op een en ander dient op de tweede vraag in zaak C-203/15 en de eerste vraag in zaak C-698/15 te worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, in die zin moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en van de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard."

6.4.2 Deze uitspraak bevat een afbakening van de gegevens waartoe toegang aan overheidsinstanties kan worden verleend, aan de hand van de kring van personen op wie die gegevens betrekking hebben. Op hoofdlijnen houdt deze rechtspraak in dat voor het doel van de bestrijding van criminaliteit de toegang aan overheidsinstanties tot gegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, in beginsel alleen mag worden verleend als het gaat om 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". Aanvullende voorwaarden daarbij zijn dat de toegang - behalve in spoedeisende gevallen - plaatsvindt na "een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit", en dat de betrokken personen, mits het belang van het onderzoek zich daartegen niet verzet, op de hoogte worden gebracht van de toegang die is verleend tot de gegevens.

Het voor het doel van de bestrijding van criminaliteit verlenen van toegang tot gegevens van anderen dan 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", is blijkens deze rechtspraak alleen toegestaan in bijzondere situaties. Daarbij wordt met name gewezen op - kort gezegd - terroristische activiteiten. Het verlenen van toegang tot de gegevens moet dan daadwerkelijk een bijdrage kunnen leveren aan de bestrijding van dergelijke activiteiten.

De vraag of de toegang tot gegevens steeds moet zijn gekoppeld aan een concrete verdenking tegen een bepaalde persoon, komt onder 6.10 nader aan de orde.

6.4.3 In de zaak Ministerio Fiscal is het Hof van Justitie nader ingegaan op, kort gezegd, de mogelijkheden om toegang aan overheidsinstanties te verlenen tot gegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, waaronder ook identificerende gegevens. Deze uitspraak houdt onder meer het volgende in:

"50 De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238), en in het arrest Tele2 Sverige en [redacted] e.a., te rechtvaardigen.

51 Wat betreft de vraag of sprake is van inmenging in die grondrechten, zij eraan herinnerd dat (...) de toegang van overheidsinstanties tot dergelijke gegevens inmenging in het in artikel 7 van het Handvest neergelegde grondrecht op eerbiediging van het privéleven vormt, zelfs al kan die inmenging om bepaalde redenen niet als „ernstig" worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Een dergelijke toegang vormt tevens inmenging in het door

artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien die toegang een verwerking van persoonsgegevens is [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak],

52 Wat betreft de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling als die in het hoofdgeding, die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, zij eraan herinnerd dat de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gegeven opsomming van doelstellingen exhaustief is, zodat die toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten (zie in die zin arrest Tele2 Sverige en [redacted] e.a., punten 90 en 115).

53 Aangaande de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, dient te worden geconstateerd dat het daarbij volgens de bewoordingen van artikel 15, lid 1, eerste zin, van richtlijn 2002/58 evenwel niet alleen over de bestrijding van ernstige delicten maar over „strafbare feiten” in het algemeen gaat.

54 Stellig heeft het Hof in dit verband geoordeeld dat ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen (zie in die zin arrest Tele2 Sverige en [redacted] e.a., punt 99).

55 Het Hof heeft die uitlegging echter gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt (zie in die zin arrest Tele2 Sverige en [redacted] e.a., punt 115).

56 Volgens het evenredigheidsbeginsel kan ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, ernstige inmenging immers slechts worden gerechtvaardigd door de doelstelling om - eveneens „ernstige” - criminaliteit te bestrijden.

57 Is de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van „strafbare feiten” in het algemeen.

58 Allereerst moet dus worden uitgemaakt of in casu, gelet op de omstandigheden van de onderhavige zaak, de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die zou voortvloeien uit het feit dat aan de gerechtelijke politie toegang tot de in het hoofdgeding aan de orde zijnde gegevens wordt verleend, als „ernstig" moet worden beschouwd.

59 In dit verband heeft het verzoek in het hoofdgeding, waarmee de gerechtelijke politie in een strafrechtelijk onderzoek via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, louter tot doel de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd. Zoals in punt 40 van het onderhavige arrest is uiteengezet, strekt dat verzoek er enkel toe om toegang te verkrijgen tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon.

60 Met de via het toegangsverzoek in het hoofdgeding beoogde gegevens is het dus blijkbaar alleen mogelijk om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

61 In die omstandigheden kan de toegang tot de in het verzoek in het hoofdgeding bedoelde gegevens niet worden aangemerkt als een „ernstige" inmenging in de grondrechten van de personen waarop de gegevens betrekking hebben.

62 Zoals uit de punten 53 tot en met 57 van dit arrest blijkt, kan de inmenging die een dergelijke gegevenstoegang zou veroorzaken dus worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 vermelde doelstelling om „strafbare feiten" in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als „ernstig" moeten worden aangemerkt.

> 63 Gelet op het voorgaande dient op de gestelde vragen te worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten - moet worden beperkt tot de bestrijding van zware criminaliteit."

Onder verwijzing naar deze rechtspraak heeft het Hof van Justitie in de zaak La Quadrature du Net e.a. onder meer het volgende overwogen:

> "157 Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als „ernstig" worden aangemerkt (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punten 59 en 60).
>
> 158 Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 62)."

Het Hof van Justitie heeft verder in de zaak Prokuratuur onder meer het volgende overwogen:

> "33 Wat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten betreft die door de in het hoofdgeding aan de orde zijnde regeling wordt nagestreefd, kunnen overeenkomstig het evenredigheidsbeginsel alleen de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid een

rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest erkende grondrechten, zoals inmengingen die voortvloeien uit de bewaring van verkeers- en locatiegegevens, ongeacht of deze algemeen en ongedifferentieerd dan wel gericht zijn. Derhalve kunnen met de door de in het hoofdgeding aan de orde zijnde regeling nagestreefde doelstelling om strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, enkel niet-ernstige inmengingen in die grondrechten worden gerechtvaardigd (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 140 en 146).

34 In dit verband is met name geoordeeld dat wettelijke maatregelen met betrekking tot de verwerking van gegevens inzake de burgerlijke identiteit van gebruikers van elektronische- communicatiemiddelen als zodanig, met name de bewaring ervan en de toegang daartoe, uitsluitend met het oog op de identificatie van de betrokken gebruiker en zonder dat deze gegevens verband kunnen houden met informatie over de verrichte communicaties, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste volzin, van richtlijn 2002/58 genoemde doelstelling om strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen. Met die gegevens alleen is het immers niet mogelijk om de datum, het tijdstip, de duur en de ontvangers van de communicaties, de plaats waar die communicaties hebben plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd te achterhalen. Zij verschaffen dus, afgezien van de contactgegevens van de gebruikers van elektronische-communicatiemiddelen, zoals hun adressen, geen enkele informatie over bepaalde communicaties en, bijgevolg, ook niet over hun persoonlijke levenssfeer. De inmenging die een maatregel strekkende tot bewaring van die gegevens met zich brengt, kan derhalve niet als „ernstig” worden aangemerkt (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 157 en 158 en aldaar aangehaalde rechtspraak).

35 In die omstandigheden kunnen alleen de doelstellingen van bestrijding van zware criminaliteit en van voorkoming van ernstige bedreigingen van de openbare veiligheid rechtvaardigen dat overheidsinstanties toegang hebben tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door die gebruiker gehanteerde eindapparatuur en op grond waarvan precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkenen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 54), zonder dat andere factoren die de evenredigheid van een verzoek om toegang bepalen, zoals de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht, tot gevolg kunnen hebben dat de doelstelling van voorkoming, onderzoek,

opsporing en vervolging van strafbare feiten in het algemeen een dergelijke toegang rechtvaardigt."

6.4.4 In deze rechtspraak stelt het Hof van Justitie het evenredigheidsbeginsel centraal. Als overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang willen verkrijgen tot gegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, speelt de ernst van de inmenging in de betrokken grondrechten een belangrijke rol. Daarbij gaat het in het bijzonder om de inmenging in het recht op eerbiediging van het privéleven. De rechtspraak van het Hof van Justitie houdt daarbij in de kern in dat een ernstige inmenging alleen kan worden gerechtvaardigd door de doelstelling om "ernstige criminaliteit" te bestrijden. Als het verlenen van toegang tot de gegevens echter niet een ernstige inmenging veroorzaakt, kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten in het algemeen, dus ook strafbare feiten die zich niet laten aanmerken als "ernstige criminaliteit".[22]

Tegen deze achtergrond is in de hiervoor weergegeven rechtspraak overwogen dat het verlenen van toegang tot uitsluitend identificerende gegevens[23] mogelijk is met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, zonder dat dus de eis wordt gesteld dat het alleen kan gaan om ernstige strafbare feiten. Van dergelijke gegevens is in ieder geval sprake als het gaat om gegevens aan de hand waarvan de betrokken gebruiker kan worden geïdentificeerd, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie.[24] Dergelijke gegevens verschaffen dan immers geen nauwkeurige informatie over het privéleven van de betrokken gebruiker. Het verlenen van toegang tot die gegevens veroorzaakt daarom niet een ernstige inmenging in met name het recht op bescherming van het privéleven. Dat verklaart ook waarom voor deze uitsluitend identificerende gegevens in de rechtspraak van het Hof van Justitie de onder 6.4.2 genoemde aanvullende voorwaarden van "voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit", en de notificatie van de betrokken personen niet worden gesteld.

6.4.5 De bepalingen van het Wetboek van Strafvordering met betrekking tot het vorderen van verkeers- en locatiegegevens alsmede identificerende gegevens

22 Zie in het bijzonder Ministerio Fiscal, overwegingen 56 en 57.

23 Hoewel – waar het gaat om e-mailverkeer en internettelefonie – IP-adressen van de bron van de communicatie, en niet van de ontvanger, van minder gevoelige aard zijn dan verkeersgegevens, kunnen dergelijke IPadressen niet op één lijn worden gesteld met identificerende gegevens. Vgl. Quadrature, overwegingen 152-156.

24 Zie onder meer Prokuratuur, overweging 34.

moeten zo veel mogelijk worden uitgelegd in overeenstemming met Richtlijn 2002/58/EG, waarbij moet worden uitgegaan van de interpretatie die het Hof van Justitie heeft gegeven aan de voorschriften van deze richtlijn. Waar het gaat om de bevoegdheden die betrekking hebben op het vorderen van uitsluitend identificerende gegevens, volgt uit het voorgaande dat Richtlijn 2002/58/EG geen aanvullende voorwaarden met zich brengt. Waar het gaat om de wettelijke bevoegdheden die betrekking hebben op het vorderen van verkeers- en locatiegegevens anders dan uitsluitend identificerende gegevens,[25] geldt dat - gelet op het evenredigheidsbeginsel - acht moet worden geslagen op de ernst van de inmenging in (met name) het recht op eerbiediging van het privéleven. Als de toepassing van die bevoegdheden een ernstige inmenging veroorzaakt, is vereist dat sprake is van "ernstige criminaliteit" (en dus ernstige strafbare feiten) en dat toepassing van die bevoegdheden plaatsvindt na "voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit".

De rechtspraak van het Hof van Justitie hierover en de daarin gehanteerde begrippen roepen vragen op over (i) de ernst van de inmenging in (met name) het recht op bescherming van het privéleven die aan de orde is of kan zijn bij het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens), en (ii) de afbakening van de begrippen "ernstige strafbare feiten" en "ernstige criminaliteit". Deze vragen komen hierna onder 6.5-6.9 nader aan de orde. In 6.10 wordt vervolgens ingegaan op de afbakening van de kring van personen op wie de gegevens betrekking hebben waartoe toegang kan worden verleend.

Precieze conclusies over de persoonlijke levenssfeer; ernstige strafbare feiten en ernstige criminaliteit

6.5.1 Zoals onder 6.4.5 is overwogen, kan uit de rechtspraak van het Hof van Justitie worden afgeleid dat als de toepassing van wettelijke bevoegdheden die betrekking hebben op verkeers- en locatiegegevens met zich brengt dat sprake is van een ernstige inmenging in met name het recht op bescherming van het privéleven, die inmenging in het licht van het evenredigheidsbeginsel alleen kan worden gerechtvaardigd als sprake is van ernstige criminaliteit (en dus ernstige strafbare feiten). De advocaat-generaal stelt in zijn vordering de voor de rechtspraktijk belangrijke vraag aan de orde of in het licht van de rechtspraak van het Hof van Justitie het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) ook kan zijn toegestaan als geen

[25] Het vorderen van gegevens op grond van artikel 126n, 126u en 126zh Sv strekt zich uit tot verkeers- en locatiegegevens, maar zou in een concreet geval op zich ook beperkt kunnen blijven tot identificerende gegevens. Immers, de gegevens waarop artikel 126n, 126u en 126zh Sv ziet, omvatten – zo volgt uit artikel 2 Besluit vorderen gegevens telecommunicatie – mede de gegevens die worden genoemd in artikel 126na, 126ua en 126zi Sv.

sprake is van ernstige strafbare feiten of ernstige criminaliteit, en wel als het in het concrete geval gaat om verkeers- en locatiegegevens waarvan de kennisneming - naar verwachting - slechts een geringe inmenging in het recht op bescherming van het privéleven zal veroorzaken. In de vordering van de advocaat-generaal wordt in het bijzonder gewezen op de uitspraak van het Hof van Justitie in de zaak Prokuratuur. Het antwoord van het Hof van Justitie op de in die zaak gestelde eerste prejudiciële vraag luidt:

"Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische- communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer - welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid -, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn."

6.5.2 De advocaat-generaal bespreekt in zijn vordering onder 97-110 op welke wijze de rechtspraak van het Hof van Justitie over de hiervoor genoemde vraag kan worden uitgelegd. Hij wijst erop dat deze rechtspraak niet eenduidig is, in die zin dat aanknopingspunten kunnen worden gevonden voor meerdere lezingen van deze rechtspraak. Het gaat dan allereerst om een lezing die ertoe strekt dat het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) alleen mogelijk is in geval van ernstige strafbare feiten of ernstige criminaliteit.[26] Een andere, tweede lezing is dat de toegang tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) ook mag worden verleend bij minder ernstige strafbare feiten of minder ernstige

[26] Ofwel omdat moet worden aangenomen dat elke raadpleging van die verkeers- en locatiegegevens een ernstige inmenging veroorzaakt in met name het recht op bescherming van het privéleven van de gebruiker, ofwel omdat het voor het verlenen van toegang tot die verkeers- en locatiegegevens geen verschil maakt of het in het concrete geval gaat om gegevens waaruit precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de gebruiker.

criminaliteit, als het verlenen van toegang tot die gegevens slechts een geringe inmenging veroorzaakt in met name het recht op bescherming van het privéleven van de gebruiker.

6.5.3 Naar het oordeel van de Hoge Raad geven de overwegingen in de rechtspraak van het Hof van Justitie over het evenredigheidsbeginsel steun aan de hiervoor genoemde tweede lezing. Zoals onder 6.4.4 is besproken, geldt op grond van het evenredigheidsbeginsel dat de toegang aan overheidsinstanties tot de gegevens die door een aanbieder van een telecommunicatiedienst worden bewaard, kan worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten in het algemeen, als het verlenen van die toegang in het concrete geval niet een inmenging of niet een ernstige inmenging in (met name) het recht op bescherming van het privéleven tot gevolg heeft.[27] Het evenredigheidsbeginsel verzet zich in dat geval dus niet tegen het verlenen van die toegang als sprake is van een strafbaar feit in het algemeen, zonder dat dit feit als "ernstig" in de hiervoor bedoelde zin kan worden aangemerkt.

Als het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens wel een ernstige inmenging veroorzaakt in (met name) het recht op bescherming van het privéleven omdat die gegevens zodanige informatie kunnen verschaffen over de communicatie door een gebruiker of de locaties van de door hem gebruikte apparatuur dat precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer, kan die inmenging alleen worden gerechtvaardigd door de doelstelling van de bestrijding van ernstige criminaliteit. De enkele omstandigheid dat het gaat om een beperkte hoeveelheid gegevens waartoe toegang wordt verleend of dat het verlenen van toegang een beperkte periode betreft waarbinnen de gegevens zijn vastgelegd, maakt dat niet anders. Beslissend is de ernst van de inmenging op met name het recht op bescherming van het privéleven. De Hoge Raad wijst in dit verband nogmaals op de navolgende overweging van het Hof van Justitie in de zaak Prokuratuur:

> "35 In die omstandigheden kunnen alleen de doelstellingen van bestrijding van zware criminaliteit en van voorkoming van ernstige bedreigingen van de openbare veiligheid rechtvaardigen dat overheidsinstanties toegang hebben tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door die gebruiker gehanteerde eindapparatuur en op grond waarvan precieze conclusies

[27] Omdat het gaat om een geval waarin aan de hand van de te verkrijgen gegevens niet of slechts in beperkte mate informatie over het privéleven van een specifieke persoon wordt verkregen. Een voorbeeld daarvan is het geval waarin nog geen concrete verdachte in beeld is en het verlenen van toegang tot gegevens zich beperkt tot de vraag welke telecommunicatie-apparatuur een zendmast op een bepaalde locatie heeft aangestraald in een zeker tijdsbestek.

> kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkenen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 54), zonder dat andere factoren die de evenredigheid van een verzoek om toegang bepalen, zoals de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht, tot gevolg kunnen hebben dat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten in het algemeen een dergelijke toegang rechtvaardigt."

6.6.1 Een vraagpunt dat in relatie tot de rechtspraak van het Hof van Justitie rijst, betreft de begrippen "ernstig strafbaar feit" en "ernstige criminaliteit" (of "zware criminaliteit"). In de onder 5.7 en 5.8 genoemde rechtspraak van het Hof van Justitie is geen nadere invulling gegeven aan die begrippen. De vraag rijst of het aan de bevoegde instanties van de lidstaten is om zelf mede invulling te geven aan deze begrippen, dan wel of het hier gaat om autonome begrippen van Unierecht.

6.6.2 In dit verband kan allereerst erop worden gewezen dat Richtlijn 2002/58/EG uitsluitend in artikel 15 lid 1 spreekt van "het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten", zonder dat daarbij een nadere invulling wordt gegeven aan het begrip "strafbare feiten". In Richtlijn 2002/58/EG komen de in de rechtspraak van het Hof van Justitie genoemde begrippen "ernstige strafbare feiten" en "ernstige criminaliteit" niet voor. Uit Richtlijn 2002/58/EG - en in het bijzonder uit artikel 1 van deze richtlijn - blijkt niet dat harmonisatie wordt beoogd van de begrippen "strafbare feiten", "ernstige strafbare feiten" en "ernstige criminaliteit". Richtlijn 2002/58/EG wijkt in dit opzicht af van bijvoorbeeld Kaderbesluit 2002/584/JBZ betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten. In dat kaderbesluit is een specifieke omschrijving opgenomen van de strafbare feiten ten aanzien waarvan overlevering mogelijk is zonder toetsing van de zogenoemde dubbele strafbaarheid van het feit.

Van belang is verder de onder 6.4.1 geciteerde rechtspraak van het Hof van Justitie over het verlenen van toegang tot verkeers- en locatiegegevens. Daarin wordt overwogen dat het aan de verwijzende rechterlijke instanties is om na te gaan of en in welke mate de nationale regelingen over onder meer de toegang van de bevoegde nationale autoriteiten tot bewaarde gegevens voldoen aan de eisen die voortvloeien uit artikel 15 lid 1 Richtlijn 2002/58/EG.[28] Dit duidt erop dat het aan de betreffende instanties van de lidstaten is om nader te bepalen of sprake is van "ernstige strafbare feiten" en "ernstige criminaliteit". In de rechtspraak van het Hof van Justitie worden ook geen gezichtspunten of criteria benoemd die van belang worden geacht

[28] Tele2, overweging 124.

wanneer in een concreet geval de vraag moet worden beantwoord of van een ernstig strafbaar feit of ernstige criminaliteit sprake is.[29]

6.6.3 Naar het oordeel van de Hoge Raad moet dan ook worden aangenomen dat de begrippen "ernstige strafbare feiten" en "ernstige criminaliteit" in de rechtspraak van het Hof van Justitie geen autonome begrippen van Unierecht vormen.[30] Wel moeten, zo kan aan die rechtspraak worden ontleend, de nationale instanties die toepassing geven aan de bevoegdheden op grond waarvan toegang wordt verleend aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens), zich ervan rekenschap geven dat die toepassing in het concrete geval verenigbaar moet zijn met de in het Handvest neergelegde rechten op eerbiediging van het privéleven, bescherming van persoonsgegevens en vrijheid van meningsuiting en van informatie. Dat betekent, zoals hiervoor al is besproken, dat de inmenging die plaatsvindt in die door het Handvest gewaarborgde rechten, in het concrete geval moet worden gerechtvaardigd door de ernst van het (vermoedelijke) strafbare feit dat aanleiding vormt voor de toepassing van de bevoegdheid. Daarbij gaat het allereerst om de ernst van het strafbare feit in algemene zin, zoals die met name blijkt uit het wettelijk strafmaximum. Daarnaast is van belang de ernst van het (vermoedelijke) strafbare feit zoals dat zich concreet heeft voorgedaan. Die ernst moet in verhouding staan tot de inmenging die plaatsvindt in met name het recht op bescherming van het privéleven.

6.7 De rechtspraak van het Hof van Justitie laat, zoals onder 6.5.2 is besproken, meerdere lezingen toe met betrekking tot de vraag of het verlenen van toegang tot verkeers- en locatiegegevens onder omstandigheden ook is toegelaten in geval van niet-ernstige criminaliteit. Daarnaast is in de rechtspraak van het Hof van Justitie tot op heden niet bevestigd dat, zoals door de Hoge Raad onder 6.6.3 is geoordeeld, het aan de bevoegde nationale autoriteiten is om zelf mede invulling te geven aan de begrippen "ernstige strafbare feiten" en "ernstige criminaliteit". Er bestaat daarom aanleiding voor het stellen van prejudiciële vragen aan het Hof van Justitie met het oog op het verkrijgen van verduidelijking van de onder 6.5 en 6.6 besproken rechtspraak. Daarbij kan het volgende worden opgemerkt over het belang van het stellen van die prejudiciële vragen voor de toepassing van het nationale recht.

6.8.1 Voor de toepassing van de bevoegdheden in het Wetboek van Strafvordering met betrekking tot het vorderen van verkeers- en locatiegegevens is - anders dan voor het vorderen van uitsluitend identificerende gegevens op grond van

[29] Vgl. over mogelijke beoordelingscriteria de conclusie van advocaat-generaal Saugmandsgaard Øe in zaak Ministerio Fiscal, onder 105.

[30] In deze zin ook de conclusie van advocaat-generaal Saugmandsgaard Øe in zaak Ministerio Fiscal, onder 100, en de conclusie van advocaat-generaal Pitruzzella in de zaak Prokuratuur, onder 91.

artikel 126na, 126ua en 126zi Sv - het enkele bestaan van een verdenking van een misdrijf niet toereikend. Voor de toepassing van de hiertoe strekkende bevoegdheden is namelijk vereist dat de verdenking betrekking heeft op een misdrijf als bedoeld in artikel 67 lid 1 Sv, dan wel dat een redelijk vermoeden bestaat dat in georganiseerd verband misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, dan wel dat aanwijzingen bestaan van een terroristisch misdrijf. Daarbij wordt met een misdrijf of misdrijven als bedoeld in artikel 67 lid 1 Sv verwezen naar de in die wettelijke bepaling opgenomen opsomming van misdrijven. Deze opsomming omvat allereerst de misdrijven waarop een maximumgevangenisstraf van vier jaren of meer is gesteld, en daarnaast een lijst van specifieke misdrijven uit het Wetboek van Strafrecht en uit bijzondere wetgeving. Een en ander betekent dat die hiervoor genoemde bevoegdheden niet kunnen worden toegepast in verband met alle misdrijven, maar alleen als het gaat om misdrijven die door de wetgever vanwege hun aard en ernst in de opsomming van artikel 67 lid 1 Sv zijn opgenomen en die dus - naar het oordeel van de Hoge Raad - moeten worden beschouwd als misdrijven die in algemene zin als “ernstig”, zoals bedoeld in de rechtspraak van het Hof van Justitie, zijn te beschouwen. Daarnaast is ook, zoals onder 6.8.3 nader aan de orde komt, de ernst van het concrete strafbare feit van belang.

6.8.2 Met betrekking tot de onder 6.3.3 en 6.3.4 besproken spoedbewaring kan erop worden gewezen dat op grond van artikel 126ni, 126ui en 126zja Sv is vereist dat sprake is van een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane strafbare feiten een ernstige inbreuk op de rechtsorde oplevert, dan wel een redelijk vermoeden bestaat dat in georganiseerd verband misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, dan wel aanwijzingen bestaan van een terroristisch misdrijf. Waar het gaat om de bevoegdheid om de verstrekking van toekomstige gegevens te vorderen, gelden de al onder 6.8.1 genoemde eisen. Ook voor de onder 6.3.3 en 6.3.4 besproken spoedbewaring geldt dus dat de betreffende bevoegdheden alleen kunnen worden toegepast in verband met misdrijven die door de wetgever vanwege hun aard en ernst in de opsomming van artikel 67 lid 1 Sv zijn opgenomen.

6.8.3 Bij de toepassing van de hiervoor besproken bevoegdheden die ertoe strekken dat in het kader van een strafvorderlijk onderzoek toegang wordt verleend tot verkeers- en locatiegegevens, moet worden voldaan aan in het bijzonder de algemene strafvorderlijke eis van proportionaliteit. Die eis brengt met zich dat het concrete strafbare feit dat voorwerp is van het redelijk vermoeden of de aanwijzingen, zo ernstig moet zijn dat de

toepassing van de bevoegdheid om verkeers- en locatiegegevens te vorderen, is gerechtvaardigd. Degene die beslist over de toepassing van de bevoegdheid, moet dit van tevoren beoordelen. Bij deze toets moet dus worden betrokken in welke mate met het verkrijgen van verkeers- en locatiegegevens (mogelijk) inbreuk wordt gemaakt op de persoonlijke levenssfeer van de gebruiker en hoe die inbreuk zich verhoudt tot de ernst van het strafbare feit zoals dat zich concreet heeft voorgedaan.

De Hoge Raad wijst er in dit verband op dat het weliswaar mogelijk is om op een abstract niveau een scheidslijn te trekken tussen strafbare feiten die ernstig zijn en strafbare feiten die niet ernstig zijn, maar dat de ernst van het concrete strafbare feit sterk kan variëren. Ook staat niet steeds tevoren exact vast of en, zo ja, welke gegevens zullen worden verkregen wanneer de verstrekking van een bepaald type gegevens wordt gevorderd, wat de inhoud van die gegevens zal zijn en op welke personen die gegevens eventueel ook naast de gebruiker betrekking zullen hebben. Bij de beoordeling of de toepassing van een bevoegdheid op grond waarvan verkeers- of locatiegegevens kunnen worden verkregen, in overeenstemming is met het recht op bescherming van het privéleven, gaat het dan ook om een inschatting en vervolgens een weging van een samenstel van factoren.[31] Onder die factoren vallen de ernst van het strafbare feit in algemene zin, de ernst van het concrete strafbare feit waarop de verdenking betrekking heeft, de gegevens die - gelet op de wijze waarop de vordering wordt geformuleerd en afgebakend - waarschijnlijk zullen (kunnen) worden verkregen over de gebruiker en eventueel ook andere personen, het belang van het verkrijgen van die gegevens voor het strafrechtelijke onderzoek en de vraag of en, zo ja, in welke mate aan de hand van die gegevens conclusies kunnen worden getrokken over het privéleven. Hierbinnen bestaat in zekere zin een glijdende schaal: naarmate de (te verwachten) inbreuk op het recht op bescherming van het privéleven van de gebruiker groter zal zijn, mogen zwaardere eisen worden gesteld aan de ernst van het concrete strafbare feit. Andere factoren die nog een rol spelen, betreffen de wettelijke garanties die bestaan dat de gegevens die worden verkregen, niet anders worden gebruikt dan voor het strafvorderlijke onderzoek, en de voorschriften met betrekking tot de bewaring en de vernietiging van de verkregen gegevens.

6.9 Gelet op het voorgaande waarborgt een juiste toepassing van de bevoegdheden in het Wetboek van Strafvordering dat het resultaat daarvan in overeenstemming is met Richtlijn 2002/58/EG en het evenredigheidsbeginsel. De Hoge Raad gaat er daarbij van uit dat de rechtspraak van het Hof van Justitie kan worden geduid op de wijze als hiervoor onder 6.5.3 en 6.6.3 is uiteengezet. Het stellen van prejudiciële vragen aan het Hof van Justitie strekt er daarbij toe om ten behoeve van de rechtspraktijk op dit punt zekerheid te verkrijgen.

31 Vgl. Prokuratuur, overweging 40.

Zoals onder 6.6.1 is besproken, is in de rechtspraak van het Hof van Justitie vooralsnog niet bevestigd dat het aan de bevoegde nationale autoriteiten is om nader invulling te geven aan de begrippen “ernstige strafbare feiten” en “ernstige criminaliteit”. Mocht het zo zijn dat het, anders dan onder 6.6.3 door de Hoge Raad is geoordeeld, hierbij gaat om autonome begrippen van Unierecht, dan is het van belang te weten op welke wijze aan die begrippen invulling moet worden gegeven om te kunnen bepalen of en, zo ja, op welke manier, de bevoegdheden in het Wetboek van Strafvordering zich in overeenstemming met Richtlijn 2002/58/EG laten toepassen. Daarnaast is het van belang om duidelijkheid te verkrijgen over het onder 6.5 besproken vraagstuk of het verlenen van toegang tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) al dan niet zou zijn beperkt tot gevallen van ernstige criminaliteit. Ook dit vraagstuk houdt verband met het belang en de betekenis van het evenredigheidsbeginsel voor de wijze van normering van de toegang tot de door aanbieders van elektronische-communicatiediensten bewaarde gegevens.

Kring van personen

6.10.1 In de uitspraak Tele2 Sverige en [redacted] wordt, zoals onder 6.4.2 aan de orde is gekomen, overwogen dat aan de hand van objectieve criteria moet worden bepaald of toegang kan worden verleend aan overheidsinstanties tot gegevens die door aanbieders van elektronische-communicatiediensten worden bewaard. Daarbij 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 geweest bij een dergelijk misdrijf”. Toegang tot de gegevens van andere personen zou kunnen worden verleend “in bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd (...), wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren.”[32]

6.10.2 Deze rechtspraak van het Hof van Justitie kan op het eerste gezicht de vraag doen rijzen of - buiten de door het Hof van Justitie genoemde bijzondere situaties - uitsluitend aan overheidsinstanties toegang kan worden verleend tot gegevens, waaronder ook verkeers- en locatiegegevens, als deze gegevens betrekking hebben op, kort gezegd, een persoon ten aanzien van wie een verdenking bestaat. Het hanteren van zo’n vereiste kan het onderzoeken, opsporen en vervolgen van strafbare feiten in aanzienlijke

[32] Overweging 119.

mate belemmeren.[33] Zo kan de aanleiding voor het vorderen van verkeers- en locatiegegevens juist zijn dat de autoriteiten de (vermoedelijke) dader van het strafbare feit trachten te achterhalen of dat zij proberen zicht te krijgen op de wijze waarop het strafbare feit is verlopen. Voor het strafrechtelijk onderzoek kunnen belangrijke aanknopingspunten zijn gelegen in informatie over telefoonnummers die zijn gebruikt, identificatienummers van telefoontoestellen, zendmasten waarmee toestellen in verbinding hebben gestaan of IP- adressen die verband houden met elektronische vormen van communicatie. Een effectieve opsporing vergt dat gegevens kunnen worden verkregen die dan (nog) niet zijn gekoppeld aan specifieke personen en waarbij aan de te verkrijgen gegevens veelal ook nog niet of slechts in zeer beperkte mate informatie over het privéleven van personen is te ontlenen. Voor het verkrijgen van dergelijke gegevens zijn politie en justitie aangewezen op de inzet van de bevoegdheden tot het vorderen van verkeers- en locatiegegevens, ook in gevallen waarin de verdenking van een strafbaar feit nog niet concreet betrekking heeft op een specifieke persoon.

6.10.3 Om de navolgende redenen moet worden aangenomen dat de uitoefening van de bevoegdheden tot het vorderen van verkeers- en locatiegegevens - ook buiten de onder 6.10.1 genoemde uitzonderingen - niet steeds beperkt hoeft te blijven tot te individualiseren personen die als verdachte kunnen worden aangemerkt.

Allereerst is van belang dat het Hof van Justitie in zijn uitspraak in de zaak Tele2 Sverige en [redacted] verwijst naar de uitspraak van het Europees hof voor de rechten van de mens (hierna: EHRM) van 4 december 2015, nr. 47143/06 ([redacted] Rusland). In deze zaak gaat het om een klacht die betrekking heeft op, kort gezegd, het mogelijk aftappen van mobiel telefoonverkeer (“covert interception of mobile telephone Communications”). Het EHRM zet in deze uitspraak de “general principles” uiteen met betrekking tot de toelaatbaarheid van “secret surveillance measures”. Overweging 260 van deze uitspraak van het EHRM, waarnaar het Hof van Justitie specifiek verwijst, houdt het volgende in:

“Turning now to the authorisation authority’s scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of “necessity in a democratic society”, as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the

[33] Hierbij kunnen ook zogenoemde positieve verplichtingen van belang zijn. Vgl. onder meer Quadrature, overwegingen 126-128.

aims by less restrictive means (see Klass and Others, cited above, § 51; Association for European Integration and Human Rights and Ekimdzhiev, cited above, §§ 79 and 80; lordachi and Others, cited above, § 51; and Kennedy, cited above, §§ 31 and 32).”

Bij het verlenen van toegang tot verkeers- en locatiegegevens gaat het op zich niet om de interceptie van telecommunicatie. Kennelijk moet aan deze overweging van het EHRM worden ontleend dat als de toepassing van de opsporingsmethoden waarmee op heimelijke wijze informatie kan worden verkregen die is gerelateerd aan telecommunicatieverkeer, zich richt op een specifieke persoon, artikel 8 lid 2 EVRM met zich brengt dat tegen deze persoon een verdenking moet bestaan en dat het daarbij moet gaan om een verdenking met betrekking tot strafbare feiten van een zodanige ernst en aard dat de inzet van dergelijke heimelijke opsporingsmethoden is gerechtvaardigd. Daarin is een eis van proportionaliteit gelegen. Daarnaast volgt uit die overweging - in aanmerking genomen dat een inbreuk op de persoonlijke levenssfeer noodzakelijk moet zijn in een democratische samenleving - ook een eis van subsidiariteit, in die zin dat als op minder ingrijpende wijze informatie kan worden vergaard, daarvoor moet worden gekozen. Uit deze overweging van het EHRM volgt echter niet dat de toepassing van de daarin genoemde opsporingsmethoden pas is toegestaan als de verdenking van een strafbaar feit concreet betrekking heeft op een specifieke persoon. Ook volgt daaruit niet dat, als er wel concreet een verdachte in beeld is, met die opsporingsmethoden uitsluitend gegevens zouden mogen worden verkregen die betrekking hebben op die verdachte. Dergelijke beperkingen zouden ook, zoals onder 6.10.2 is opgemerkt, de mogelijkheden van opsporing en vervolging van - en daarmee de bescherming van burgers tegen - met name ernstige vormen van criminaliteit verkorten.

Daarnaast moet acht worden geslagen op de rechtspraak van het Hof van Justitie over het bewaren van gegevens door aanbieders van elektronische-communicatiediensten. Het ligt immers niet voor de hand dat bepaalde typen gegevens zoals verkeers- en locatiegegevens wel zouden mogen (of moeten) worden bewaard, maar dat het verlenen van toegang daartoe (in het geheel) niet zou zijn toegestaan. Uit de uitspraak in de zaak Tele2 Sverige en [redacted] kan worden afgeleid dat een bewaarplicht in overeenstemming is met Richtlijn 2002/58/EG wanneer deze zich beperkt tot “gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij de bestrijding van criminaliteit”.[34] Waar het gaat om de spoedbewaring van verkeers- en locatiegegevens blijkt uit de uitspraak van het Hof van Justitie

[34] Overweging 106. Zie daarnaast Quadrature, overwegingen 147-150.

in de zaak La Quadrature du Net e.a. dat spoedbewaring "niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht". Verder overweegt het Hof van Justitie in diezelfde uitspraak dat spoedbewaring "naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke [kan] worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd."[35] Tot de hier omschreven gegevens mag ook, onder de hiervoor al besproken voorwaarden, toegang worden verleend.[36]

6.10.4 Uit een en ander volgt dat het verlenen van toegang aan overheidsinstanties op grond van Richtlijn 2002/58/EG zich niet beperkt tot door aanbieders van elektronische- communicatiediensten bewaarde gegevens die betrekking hebben op, kort gezegd, een persoon ten aanzien van wie een verdenking bestaat. Daarbij geldt wel dat ook moet worden voldaan aan de eisen van proportionaliteit en subsidiariteit. Dat betekent dat, zoals ook onder 6.4.4 is besproken, als het verlenen van toegang tot gegevens een ernstige inmenging oplevert in het recht op bescherming van het privéleven, deze toegang alleen wordt verleend met het oog op de bestrijding van ernstige criminaliteit. Daarnaast moet bij de beslissing of die toegang wordt verleend, in aanmerking worden genomen of de benodigde informatie mogelijk op minder ingrijpende wijze kan worden vergaard.

Toetsing voorafgaand aan de toepassing van de bevoegdheden in het Wetboek van Strafvordering

6.11.1 Zoals onder 6.4.5 is besproken, brengt de rechtspraak van het Hof van Justitie bij de huidige stand van zaken met zich dat - behalve in spoedeisende gevallen - de toegang tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) alleen plaatsvindt na "een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit", als de toepassing van de betreffende bevoegdheid een ernstige inmenging in het recht op bescherming van het

35 Overweging 165.

36 Overwegingen 166-167.

privéleven van de gebruiker met zich brengt. Dat voorafgaande toezicht is niet vereist wanneer het uitsluitend gaat om het verlenen van toegang tot gegevens aan de hand waarvan de betrokken gebruiker kan worden geïdentificeerd, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie.

In de zaak Prokuratuur is het Hof van Justitie ingegaan op de vraag of dit voorafgaande toezicht ook kan worden uitgeoefend door een openbaar aanklager. De volgende overwegingen zijn hierbij van belang:

> "51 (...) [Het is] van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan voorafgaande toetsing 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 instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 189 en aldaar aangehaalde rechtspraak).
>
> 52 Die voorafgaande toetsing vereist onder meer, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 105 van zijn conclusie, dat de rechterlijke instantie of de entiteit die belast is met die toetsing, over alle bevoegdheden beschikt en alle noodzakelijke waarborgen biedt om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die rechterlijke instantie of entiteit in staat is een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft.
>
> 53 Wanneer een dergelijke toetsing niet door een rechterlijke instantie maar door een onafhankelijke bestuurlijke entiteit wordt uitgeoefend, moet deze laatste een zodanige status hebben dat zij bij de uitoefening van haar taken objectief en onpartijdig kan handelen, en moet zij daartoe vrij zijn van elke invloed van buitenaf [zie in die zin arrest van 9 maart 2010, Commissie/Duitsland, C-518/07, EU:C:2010:125, punt 25, en advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 229 en 230],

54 Uit de voorgaande overwegingen volgt dat het vereiste van onafhankelijkheid waaraan moet worden voldaan door de instantie die de in punt 51 van het onderhavige arrest in herinnering gebrachte voorafgaande toetsing moet verrichten, impliceert dat deze instantie de hoedanigheid van derde moet hebben ten opzichte van degene die om toegang tot de gegevens verzoekt, zodat eerstgenoemde de toetsing objectief en onpartijdig en zonder beïnvloeding van buitenaf kan verrichten. In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied, zoals de advocaat-generaal in wezen in punt 126 van zijn conclusie heeft opgemerkt, dat de instantie die belast is met die voorafgaande toetsing enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en anderzijds neutraal moet zijn ten opzichte van de partijen in de strafprocedure.

55 Dat is niet het geval bij een openbaar ministerie dat de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager. Het openbaar ministerie heeft immers niet tot taak om een geschil in volledige onafhankelijkheid te beslechten, maar om het, in voorkomend geval, als procespartij die de strafvordering instelt, voor te leggen aan de bevoegde rechter.

56 De omstandigheid dat het openbaar ministerie overeenkomstig de regels inzake zijn bevoegdheden en zijn statuut gehouden is om de belastende en ontlastende elementen te onderzoeken, de rechtmatigheid van de onderzoeksprocedure te waarborgen en uitsluitend op te treden in overeenstemming met de wet en zijn eigen overtuiging, kan niet volstaan om het ten aanzien van de betrokken belangen de hoedanigheid van derde in de zin van punt 52 van het onderhavige arrest te verlenen.

57 Hieruit volgt dat het openbaar ministerie niet in staat is om de in punt 51 van het onderhavige arrest bedoelde voorafgaande toetsing te verrichten.

58 Aangezien de verwijzende rechter bovendien de vraag heeft opgeworpen of het ontbreken van controle door een onafhankelijke instantie kan worden verholpen aan de hand van een latere, door een rechterlijke instantie verrichte toetsing van de rechtmatigheid van de toegang van een nationale instantie tot verkeers- en locatiegegevens, moet worden opgemerkt dat de onafhankelijke toetsing, zoals de in punt 51 van het onderhavige arrest in herinnering gebrachte rechtspraak vereist, voorafgaand aan elke toegang moet plaatsvinden, behalve in naar behoren gemotiveerde urgente gevallen. In laatstgenoemde gevallen dient de toetsing op korte termijn plaats te vinden. Zoals de advocaat-generaal in punt 128 van zijn conclusie heeft vastgesteld, kan met een dergelijke latere toetsing niet worden

tegemoetgekomen aan het doel van een voorafgaande toetsing, dat erin bestaat te verhinderen dat tot de betrokken gegevens een toegang wordt verleend die verder gaat dan strikt noodzakelijk is.

59 In die omstandigheden moet op de derde prejudiciële vraag worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die het openbaar ministerie, dat tot taak heeft de strafprocedure in te leiden en, in voorkomend geval, in een latere procedure op te treden als openbaar aanklager, de bevoegdheid toekent om een overheidsinstantie ten behoeve van een strafrechtelijk onderzoek toegang te verlenen tot verkeers- en locatiegegevens."

6.11.2 Uit deze rechtspraak van het Hof van Justitie vloeit voort dat de toepassing van de in het Wetboek van Strafvordering neergelegde bevoegdheden tot het vorderen van verkeers- en locatiegegevens, niet in overeenstemming is met de eisen die Richtlijn 2002/58/EG stelt, als de toepassing van de betreffende bevoegdheid met zich brengt dat sprake is van een ernstige inmenging in het recht op bescherming van het privéleven en de beslissing tot de toepassing van die bevoegdheid wordt genomen door de officier van justitie. De vraag rijst daarom of (het stelsel van) de wet ruimte laat voor een andere wijze van uitoefening van deze bevoegdheden tot het vorderen van verkeers- en locatiegegevens die wel in overeenstemming is met die eisen.

6.11.3 De advocaat-generaal heeft in zijn vordering onder 117-125 de systematische uitgangspunten van het Wetboek van Strafvordering met betrekking tot de rol van de rechter-commissaris in het opsporingsonderzoek beschreven. Daaruit volgt dat het stelsel van het Wetboek van Strafvordering zich niet ertegen verzet dat de officier van justitie met het oog op het uitoefenen van een bevoegdheid die ertoe strekt verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) als bedoeld in artikel 2, onder b en c, Richtlijn 2002/58/EG te verkrijgen, een machtiging van de rechtercommissaris vordert. De officier van justitie kan die machtiging dus ook vorderen in gevallen waarin het Wetboek van Strafvordering niet de eis stelt dat de officier van justitie de vordering tot het verstrekken van verkeers- en locatiegegevens pas doet nadat hij een machtiging van de rechter-commissaris heeft verkregen. In aansluiting op andere bevoegdheden met betrekking tot het vorderen van gegevens en met betrekking tot communicatie door middel van geautomatiseerde werken geldt dat de rechter-commissaris een machtiging schriftelijk verleent. In geval van dringende noodzaak kan de machtiging van de rechter-commissaris mondeling worden gegeven. In dat geval stelt de rechtercommissaris de machtiging binnen drie dagen op schrift (vgl. artikel 126nf Sv en artikel 126m lid 5 Sv, telkens in verbinding met artikel 1261 lid 7 Sv).

6.11.4 Met betrekking tot de vraag in welke gevallen de officier van justitie gehouden is een schriftelijke machtiging van de rechter-commissaris te vorderen, merkt de Hoge Raad het volgende op. Of het vorderen van verkeers- en locatiegegevens een ernstige inmenging in het recht op bescherming van het privéleven van de gebruiker veroorzaakt en, zo ja, of die inmenging in een concreet geval kan worden gerechtvaardigd, moet worden bepaald aan de hand van in het bijzonder de aard van de gegevens, het misdrijf of de misdrijven in verband waarmee de vordering wordt gedaan en de persoon of de personen op wie de te verstrekken gegevens betrekking hebben. Daarbij staat, zoals ook onder 6.8.3 is overwogen, ten tijde van het doen van de vordering niet steeds exact vast of en, zo ja, welke gegevens zullen worden verkregen en wat de inhoud van die gegevens zal zijn. Daarom kan ook niet steeds tevoren worden bepaald of een ernstige inmenging in het recht op bescherming van het privéleven van de gebruiker zal plaatsvinden.

De Hoge Raad vindt hierin aanleiding te bepalen dat als de officier van justitie verkeers- en locatiegegevens wil verkrijgen die meer omvatten dan uitsluitend identificerende gegevens, hij gehouden is een schriftelijke machtiging van de rechter-commissaris te vorderen voor het vorderen van die gegevens. Praktisch gesproken houdt dit in dat als de officier van justitie toepassing geeft aan de bevoegdheden op grond van artikel 126na, 126ua en 126zi Sv, hij geen schriftelijke machtiging van de rechter-commissaris nodig heeft. Geeft de officier van justitie daarentegen toepassing aan de bevoegdheden van artikel 126n, 126u en 126zh Sv, aan de bevoegdheden van artikel 126ni, 126ui en 126zja Sv, voor zover de vordering dan is gericht aan de aanbieder van een communicatiedienst, of aan de bevoegdheid van artikel 126zo Sv, dan moet hij - ook al schrijft de wet dat niet voor - een schriftelijke machtiging van de rechter-commissaris vorderen.

6.11.5 Als de officier van justitie een schriftelijke machtiging vordert, is de rechter-commissaris gehouden daarop te beslissen. De omstandigheid dat - naar het oordeel van de rechtercommissaris - het vorderen van de betreffende gegevens niet een (meer dan geringe) inbreuk op de persoonlijke levenssfeer van de gebruiker zal opleveren, vormt geen grond voor niet-ontvankelijkverklaring van de officier van justitie in de vordering.

Bij de beslissing over het verlenen van een machtiging beoordeelt de rechter-commissaris of er wordt voldaan aan de eisen die de wet stelt aan het doen van een vordering tot het verstrekken van verkeers- en locatiegegevens, alsmede of het doen van die vordering in overeenstemming is met de eisen van proportionaliteit en subsidiariteit, zoals hiervoor onder 6.8.1-6.8.3 alsmede 6.10.3 en 6.10.4 nader is omschreven. Daarmee is gewaarborgd dat die toetsing erop is gericht “een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de

persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft".[37]

6.11.6 Een en ander betekent dat het - anders dan de wetgever bij de totstandkoming van de betreffende bepalingen tot uitgangspunt heeft genomen - voor een richtlijnconforme toepassing van de bevoegdheden van artikel 126n, 126u en 126zh Sv, de bevoegdheden van artikel 126ni, 126ui en 126zja Sv, voor zover de vordering dan is gericht aan de aanbieder van een communicatiedienst, en de bevoegdheid van artikel 126zo Sv, noodzakelijk is dat de rechter-commissaris een toetsende rol vervult. Dat vergt dat aan de gerechten voldoende capaciteit ter beschikking wordt gesteld om hen in staat te stellen de vorderingen die de officier van justitie in dit verband zal doen, te beoordelen.

Vormverzuimen

6.12.1 Als bij de uitoefening van de onder 5.1 en 5.2 besproken bevoegdheden vormverzuimen worden begaan, rijst de vraag of aan het vormverzuim een rechtsgevolg moet worden verbonden en, zo ja, welk rechtsgevolg. Gedacht kan onder meer worden aan het geval waarin het vorderen van verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) heeft plaatsgevonden zonder dat van tevoren een machtiging van de rechter-commissaris is verkregen, terwijl die machtiging gelet op wat onder 6.11 is overwogen wel was vereist. Het antwoord op de vraag of aan zo'n verzuim een rechtsgevolg moet worden verbonden, is in het bijzonder van belang in het licht van het gegeven dat de betekenis van de voorschriften van Richtlijn 2002/58/EG door het Hof van Justitie in opeenvolgende arresten stapsgewijs is verduidelijkt. Daardoor bestaat de mogelijkheid dat zich gevallen hebben voorgedaan of zich voordoen waarin pas nadat de officier van justitie toepassing heeft gegeven aan de onder 5.1 en 5.2 besproken bevoegdheden, blijkt dat die toepassing niet in alle opzichten voldoet aan de eisen die het Unierecht stelt.

6.12.2 In de uitspraak in de zaak Prokuratuur heeft het Hof van Justitie geoordeeld dat het in beginsel uitsluitend aan het nationale recht staat om de regels vast te stellen over de toelaatbaarheid en de beoordeling in strafzaken van informatie en bewijsmateriaal die zijn verkregen door (onder meer) een met het Unierecht strijdige toegang van nationale instanties tot verkeers- en locatiegegevens.[38] Het Hof van Justitie heeft hierover verder het volgende overwogen:

"41 Ten slotte moet - gelet op het feit dat de verwijzende rechter is verzocht de op basis van verkeers- en locatiegegevens opgestelde processen-verbaal

[37] Prokuratuur, overweging 52.

[38] Prokuratuur, overweging 41.

niet toelaatbaar te verklaren omdat de bepalingen van § 1111 van de wet inzake elektronische communicatie, wat zowel de bewaring van als de toegang tot gegevens betreft, in strijd zijn met artikel 15, lid 1, van richtlijn 2002/58 - in aanmerking worden genomen dat het bij de huidige stand van het Unierecht in beginsel uitsluitend aan het nationale recht staat om de regels vast te stellen betreffende de toelaatbaarheid en de beoordeling, in het kader van strafprocedures tegen personen die van strafbare feiten worden verdacht, van informatie en bewijsmateriaal die zijn verkregen door de algemene en ongedifferentieerde bewaring van dergelijke gegevens, in strijd met het recht van de Unie (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 222), of door een met dat recht strijdige toegang van de nationale instanties tot die gegevens.

42 Volgens vaste rechtspraak is het, bij gebreke van regels van de Unie ter zake, aan de nationale rechtsorde van elke lidstaat om, overeenkomstig het beginsel van procedurele autonomie, de procedurele regelingen voor gerechtelijke procedures vast te stellen ter vrijwaring van de rechten die de justitiabelen aan het recht van de Unie ontlenen, op voorwaarde evenwel dat zij niet minder gunstig zijn dan die welke gelden voor soortgelijke situaties die onder het nationale recht vallen (gelijkwaardigheidsbeginsel) en dat zij de uitoefening van de door het recht van de Unie verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 223 en aldaar aangehaalde rechtspraak).

43 Wat meer in het bijzonder het doeltreffendheidsbeginsel betreft, zij eraan herinnerd dat de nationale regels inzake aanvaarding en gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dit doel kan volgens het nationale recht niet alleen worden bereikt door een verbod op het gebruik van dergelijke informatie en bewijselementen, maar ook door nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 225).

44 Bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, moet met name worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben. Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid

is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en moet dat bewijsmiddel uitsluiten om die schending te voorkomen. Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens dan wel via toegang daartoe door de bevoegde instantie in strijd met dit recht zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C- 511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 226 en 227).”

6.12.3 Vormverzuimen die verband houden met de toepassing van de bevoegdheden die ertoe strekken verkeers- en locatiegegevens te verkrijgen, worden beoordeeld op grond van artikel 359a Sv. De uitgangspunten van de regeling van artikel 359a Sv, zoals deze zijn ontwikkeld in de rechtspraak van de Hoge Raad,[39] sluiten aan bij de onder 6.12.2 geciteerde overwegingen van het Hof van Justitie over de betekenis van met name het doeltreffendheidsbeginsel voor de situatie waarin de toegang tot verkeers- en locatiegegevens in strijd met het Unierecht is verleend. Daarbij is van belang dat, zoals in dit verband ook door het Unierecht wordt vereist, bij de behandeling van de strafzaak de verdediging de gelegenheid heeft - en ook moet krijgen - om zich uit te laten over het bewijsmateriaal en (de rechtmatigheid van) de verkrijging daarvan.

6.12.4 Bewijsuitsluiting als aan het vormverzuim te verbinden rechtsgevolg kan allereerst in aanmerking komen als het uitsluiten van bepaalde resultaten van het opsporingsonderzoek van het gebruik voor het bewijs, noodzakelijk is om een schending van het recht op een eerlijk proces zoals gewaarborgd door artikel 6 EVRM - en het daarmee overeenkomende artikel 47 lid 2 Handvest - te voorkomen.[40] Daarnaast kan bewijsuitsluiting aan de orde zijn bij een ernstige schending van een strafvorderlijk voorschrift of rechtsbeginsel; dan kan onder omstandigheden toepassing van bewijsuitsluiting noodzakelijk worden geacht als rechtsstatelijke waarborg en als middel om met de opsporing en vervolging belaste ambtenaren te weerhouden van onrechtmatig optreden en daarmee als middel om te

39 Zie in het bijzonder HR 1 december 2020, ECLI:NL:HR:2020:1889.

40 HR 1 december 2020, ECLI:NL:HR:2020:1889, rechtsoverweging 2.4.1.

voorkomen dat vergelijkbare vormverzuimen in de toekomst zullen plaatsvinden.[41] De omstandigheid dat de officier van justitie een vordering heeft gedaan tot het verstrekken van verkeers- of locatiegegevens (anders dan uitsluitend identificerende gegevens) zonder dat tevoren een machtiging van de rechter-commissaris is verkregen, terwijl die machtiging gelet op wat onder 6.11.4 is overwogen wel was vereist, levert als zodanig geen grond op voor bewijsuitsluiting.

6.12.5 Voor toepassing van strafvermindering is vereist dat de verdachte door het vormverzuim daadwerkelijk nadeel heeft ondervonden en dat strafvermindering ook in het licht van het belang van het geschonden voorschrift en de ernst van het verzuim gerechtvaardigd is. Strafvermindering laat zich als rechtsgevolg dat geschikt is voor compensatie van door de verdachte ondervonden nadeel, verbinden aan onder meer vormverzuimen waardoor een inbreuk is gemaakt op de persoonlijke levenssfeer van de verdachte.[42] Als de officier van justitie een vordering heeft gedaan tot het verstrekken van verkeers- of locatiegegevens (anders dan uitsluitend identificerende gegevens) zonder dat van tevoren een machtiging van de rechter-commissaris is verkregen, terwijl die machtiging gelet op wat onder 6.11.4 is overwogen wel was vereist, en door het doen van die vordering bewijs is verkregen ten laste van de verdachte, kan aanleiding bestaan voor strafvermindering. De vraag of, en de mate waarin de persoonlijke levenssfeer van de verdachte is geschonden, is daarbij mede bepalend voor de ernst van het verzuim en het door het verzuim daadwerkelijk geleden nadeel. Voor de toepassing van strafvermindering moet het gaan om een voldoende ernstig vormverzuim dat concreet de belangen van de verdachte in de strafzaak heeft aangetast. Als door het vormverzuim in niet meer dan geringe mate inbreuk is gemaakt op het recht op bescherming van de persoonlijke levenssfeer, kan de rechter volstaan met de enkele constatering van dat vormverzuim.[43]

Besliskader en gevolgen voor andere strafzaken

6.13.1 Op grond van de rechtspraak van het Hof van Justitie, zoals die hiervoor is besproken, komt de Hoge Raad tot het oordeel dat de regeling van de in het Wetboek van Strafvordering neergelegde bevoegdheden tot het vorderen van verkeers- en locatiegegevens, niet in overeenstemming is met de eisen die Richtlijn 2002/58/EG stelt, als de toepassing van de betreffende bevoegdheid met zich brengt dat sprake is van een ernstige inmenging in het recht op bescherming van het privéleven en de beslissing tot de toepassing van die bevoegdheid wordt genomen door de officier van justitie. Vereist is

41 HR 1 december 2020, ECLI:NL:HR:2020:1889, rechtsoverweging 2.4.4.

42 HR 1 december 2020, ECLI:NL:HR:2020:1889, rechtsoverwegingen 2.3.2 en 2.3.4.

43 HR 1 december 2020, ECLI:NL:HR:2020:1889, rechtsoverweging 2.3.2.

dan - behalve in spoedeisende gevallen - dat “voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit” plaatsvindt. Dat toezicht kan niet worden uitgeoefend door een openbaar aanklager en dus niet door de officier van justitie. Dit voorafgaande toezicht is niet vereist wanneer het uitsluitend gaat om het verlenen van toegang tot gegevens aan de hand waarvan de betrokken gebruiker kan worden geïdentificeerd, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie.

6.13.2 De Hoge Raad vindt hierin aanleiding te bepalen dat als de officier van justitie verkeers- en locatiegegevens wil verkrijgen die meer omvatten dan uitsluitend identificerende gegevens, hij gehouden is een schriftelijke machtiging van de rechter-commissaris te vorderen voor het vorderen van die gegevens. Praktisch gesproken houdt dit in dat als de officier van justitie toepassing geeft aan de bevoegdheden op grond van artikel 126na, 126ua en 126zi Sv, hij geen schriftelijke machtiging van de rechter-commissaris nodig heeft. Geeft de officier van justitie daarentegen toepassing aan de bevoegdheden van artikel 126n, 126u en 126zh Sv, aan de bevoegdheden van artikel 126ni, 126ui en 126zja Sv, voor zover de vordering dan is gericht aan de aanbieder van een communicatiedienst, of aan de bevoegdheid van artikel 126zo Sv, dan moet hij - ook al schrijft de wet dat niet voor - een schriftelijke machtiging van de rechter-commissaris vorderen.

6.13.3 Als de officier van justitie een schriftelijke machtiging vordert, moet de rechter-commissaris daarop beslissen. Bij die beslissing beoordeelt de rechter-commissaris of er wordt voldaan aan de eisen die de wet stelt aan het doen van een vordering tot het verstrekken van verkeers- en locatiegegevens, alsmede of het doen van die vordering in overeenstemming is met de eisen van proportionaliteit en subsidiariteit.

6.13.4 Omdat er naar aanleiding van de rechtspraak van het Hof van Justitie vragen rijzen over de wijze waarop Richtlijn 2002/58/EG moet worden uitgelegd, zal de Hoge Raad prejudiciële vragen stellen aan het Hof van Justitie (zie hierna onder 8).

6.13.5 Het is - mede gelet op wat daarover in de vordering van de advocaat-generaal onder 145 en 146 is opgemerkt - niet nodig dat, in afwachting van de beantwoording van de prejudiciële vragen door het Hof van Justitie, andere zaken waarin sprake is van een vordering tot verkeers- of locatiegegevens worden aangehouden. Er kan in lopende zaken worden uitgegaan van het hiervoor door de Hoge Raad weergegeven beslissingskader.

7. Beoordeling van het cassatiemiddel

7.1 Het cassatiemiddel klaagt over het oordeel van de rechtbank dat het verlenen van een schriftelijke machtiging tot het vorderen van gegevens als bedoeld

in artikel 126n Sv in het onderhavige geval in overeenstemming is met de eisen die Richtlijn 2002/58/EG stelt aan in het bijzonder het strafbare feit in verband waarmee die gegevens mogen worden gevorderd.

7.2 De beschikking van de rechtbank heeft betrekking op een vordering tot het verstrekken van gegevens over een gebruiker (te weten: de verdachte) van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker in de periode van 9 tot en met 12 augustus 2021. Het gaat dus om een vordering tot het verstrekken van (historische) verkeers- en locatiegegevens als bedoeld in artikel 126n lid 1 Sv.

7.3 In verband met het te hanteren toetsingskader is allereerst het volgende van belang. De rechtbank heeft beoordeeld of de vordering van de officier van justitie tot het verlenen van een machtiging tot het verstrekken van verkeers- en locatiegegevens, op grond van artikel 126n Sv kan worden toegewezen. Artikel 126n lid 1 Sv vereist dat sprake is van een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv. Deze bepaling stelt - anders dan artikel 126ng lid 2 Sv - niet de eis dat dit misdrijf een ernstige inbreuk op de rechtsorde oplevert. Ook uit de rechtspraak van het Hof van Justitie volgt niet dat vastgesteld moet worden dat sprake is van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert. Aangenomen moet worden dat de verwijzing door de rechtbank, in de hiervoor onder 4.2 weergegeven overwegingen, naar het criterium dat sprake is van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, op een kennelijke misslag berust. De overwegingen van de rechtbank kunnen in zoverre verbeterd worden gelezen.

7.4.1 De rechtbank heeft geoordeeld dat de vordering tot het verstrekken van verkeers- en locatiegegevens in dit geval verband houdt met de bestrijding van zware criminaliteit. De rechtbank heeft daartoe in aanmerking genomen dat de verdenking betrekking heeft op een gekwalificeerde diefstal in vereniging, dat op dit misdrijf een maximum gevangenisstraf van zes jaren is gesteld - zodat het ook gaat om een misdrijf als omschreven in artikel 67 lid 1 Sv - en dat dit misdrijf betrekking heeft op een voorwerp met een waarde van ongeveer € 18.000. Daarnaast heeft de rechtbank in haar oordeel betrokken dat voor het misdrijf waarvan de gebruiker wordt verdacht voorlopige hechtenis is toegelaten en dat tegen de gebruiker - gelet op het gevaar voor herhaling - een bevel bewaring is verleend.

7.4.2 Uitgaande van wat hiervoor onder 6.5.3, 6.6.3 en 6.8 is overwogen, getuigt het kennelijke oordeel van de rechtbank dat, gelet op de eisen die de wet en het Unierecht stellen, een machtiging kan worden verleend tot het vorderen van verkeers- en locatiegegevens, niet van een onjuiste rechtsopvatting. Immers, een misdrijf in de zin van artikel 67 lid 1 Sv - waaronder ook een gekwalificeerde diefstal in vereniging - kan in het algemeen worden aangemerkt als een ernstig misdrijf. De rechtbank heeft daarnaast de ernst van het concrete feit waarvan de gebruiker wordt verdacht, in aanmerking

genomen. Op grond daarvan heeft zij kennelijk en niet onbegrijpelijk geoordeeld dat, in aanmerking genomen dat met het vorderen van de in artikel 126n lid 1 Sv bedoelde gegevens over de gebruiker en het communicatieverkeer met betrekking tot die gebruiker in relatie tot één telefoonnummer over een periode van vier dagen een inbreuk wordt gemaakt op het recht op bescherming van het privéleven van de betrokkene, die inbreuk in verhouding staat tot deze ernst van het concrete feit.

8. Verzoek om een prejudiciële beslissing

8.1 Zoals onder 6.2 en 6.7 nader is uiteengezet, is het aangewezen prejudiciële vragen te stellen aan het Hof van Justitie in verband met de in dit arrest besproken rechtsvragen, om een definitief oordeel te kunnen vellen over het cassatiemiddel.

8.2 De eerste prejudiciële vraag luidt:

> Vallen wettelijke maatregelen die betrekking hebben op het in verband met het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten verlenen aan overheidsinstanties van toegang tot verkeers- en locatiegegevens (met inbegrip van identificerende gegevens), onder de werkingssfeer van Richtlijn 2002/58/EG, als het gaat om het verlenen van toegang tot gegevens die niet worden bewaard op grond van wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG, maar die door de aanbieder worden bewaard op een andere grond?

Om de redenen die onder 6.2.4 zijn besproken, komt het de Hoge Raad voor dat deze vraag bevestigend moet worden beantwoord.

8.3 De tweede prejudiciële vraag luidt:

> a) Vormen de in de onder 5.7 en 5.8 genoemde arresten van het Hof van Justitie gehanteerde begrippen “ernstige strafbare feiten” en “ernstige criminaliteit” (of “zware criminaliteit”) autonome begrippen van Unierecht of is het aan de bevoegde instanties van de lidstaten om zelf mede invulling te geven aan deze begrippen?
>
> b) Als het gaat om autonome begrippen van Unierecht, op welke wijze dient dan te worden vastgesteld of sprake is van een “ernstig strafbaar feit” of van “ernstige criminaliteit”?

Om de redenen die onder 6.6.2 en 6.6.3 zijn besproken, komt het de Hoge Raad voor dat het aan de bevoegde instanties van de lidstaten is om zelf mede invulling te geven aan de genoemde begrippen.

8.4 De derde prejudiciële vraag luidt:

> Kan het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten onder Richtlijn 2002/58/EG worden toegestaan als geen sprake is van ernstige strafbare feiten of ernstige criminaliteit, namelijk als in het concrete geval het verlenen van toegang tot die gegevens - naar mag worden aangenomen - slechts een geringe inmenging veroorzaakt in met name het recht op bescherming van het privéleven van de gebruiker als bedoeld in artikel 2, onder b, Richtlijn 2002/58/EG?

Om de redenen die onder 6.5.3 zijn besproken, komt het de Hoge Raad voor dat gelet op de overwegingen in de onder 5.7 en 5.8 genoemde arresten van het Hof van Justitie over het evenredigheidsbeginsel, deze vraag bevestigend moet worden beantwoord.

8.5 Alvorens verder te beslissen verzoekt de Hoge Raad het Hof van Justitie van de Europese Unie uitspraak te doen over Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) met betrekking tot de hiervoor genoemde vragen. De Hoge Raad merkt op dat deze prejudiciële vragen worden gesteld in het kader van een cassatieprocedure in het belang van de wet. Dat de Hoge Raad ook in het kader van zo'n procedure bevoegd is prejudiciële vragen te stellen, blijkt uit het arrest van het Hof van Justitie in de zaak Procureur-Generaal bij de Hoge Raad der Nederlanden.[44]

[OMISSIS]

[OMISSIS] [Slotformule en ondertekening]

[44] HvJ EU 21 november 2019, zaak C-678/18, ECLI:EU:C:2019:998, in het bijzonder overwegingen 21-27.