Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2004–2005

26 671 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

Nr. 7

TWEEDE NOTA VAN WIJZIGING

Ontvangen 22 maart 2005

Het voorstel van wet wordt als volgt gewijzigd.

1

In het opschrift van het wetsvoorstel en in de considerans wordt «en de Telecommunicatiewet» vervangen door «en enige andere wetten».

1a

In artikel I wordt vóór onderdeel B een onderdeel ingevoegd, luidende:

A

Artikel 5, eerste lid, wordt gewijzigd als volgt:

1. Aan het slot van onderdeel 3° wordt de punt vervangen door een puntkomma.

2. Na onderdeel 3° wordt een onderdeel toegevoegd, luidende:
4°. aan een der misdrijven omschreven in de artikelen 138a, 138b, 139c, 139d, 161sexies, 225, 226, 227, 240a, 240b, 326, 326c, 350, 350a en 351, voor zover het feit valt onder de omschrijving van de artikelen 2 tot en met 10 van het op 23 november 2001 te Budapest tot stand gekomen Internationaal Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18, en 2004, 290).

2

Artikel I, onderdeel D, subonderdeel 1, komt te luiden:

1. Het eerste lid komt te luiden:
1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

KST85240
0405tkkst26671-7
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2005

a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel, of
d. door het aannemen van een valse hoedanigheid.

3

In artikel I, onderdeel E, wordt in artikel 138b «hij die opzettelijk en wederrechtelijk, door tussenkomst van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, aan een ander gegevens toezendt die zijn bestemd om diens toegang tot dat netwerk of die dienst te belemmeren» vervangen door: hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.

4

Artikel I, onderdeel F, komt te luiden:

F

Artikel 139a wordt gewijzigd als volgt:

1. Het tweede lid vervalt.
2. In het derde lid, dat wordt vernummerd tot tweede lid, wordt de aanhef vervangen door «Het eerste lid is niet van toepassing op het opnemen:» en komt onderdeel 1° te luiden:
1°. van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk;.

5

Artikel I, onderdeel G, komt te luiden:

G

Artikel 139b wordt gewijzigd als volgt:

1. Het tweede lid komt te luiden:
2. Artikel 139a, tweede lid, onder 1° en 3°, is van overeenkomstige toepassing.

2. Het derde lid vervalt.

6

Artikel I, onderdeel H, komt te luiden:

H

Artikel 139c, eerste lid, komt te luiden als volgt:
1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.

7

Artikel I, onderdeel I, komt te luiden:

I

Artikel 139d wordt gewijzigd als volgt:

1. Onder plaatsing voor de tekst van de aanduiding «1.», wordt «zes maanden» vervangen door «een jaar» en wordt na «gegevensoverdracht» ingevoegd «of andere gegevensverwerking».

2. Er worden twee leden toegevoegd, luidende:

2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138a, eerste lid, 138b of 139c wordt gepleegd:

a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of

b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden gekregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt terwijl zijn oogmerk is gericht op een misdrijf als bedoeld in artikel 138a, tweede of derde lid.

8

In artikel I wordt na onderdeel I een onderdeel ingevoegd, luidende:

Ia

In artikel 139e, onderdelen 1° en 2°, wordt na «gegevensoverdracht» telkens ingevoegd: of andere gegevensverwerking.

9

Artikel I, onderdeel J, komt te luiden:

J

Artikel 161sexies wordt gewijzigd als volgt:

1. Onder plaatsing voor de tekst van de aanduiding «1.», vervalt in de aanhef «voor opslag of verwerking van gegevens» en wordt in onderdeel 1° «zes maanden» vervangen door «een jaar» en «van de opslag of verwerking» door «van de opslag, verwerking of overdracht».

2. Er wordt een lid toegevoegd, luidende:

2. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vijfde categorie wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in het eerste lid wordt gepleegd:

a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of

b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

10

In artikel I wordt na onderdeel J een onderdeel ingevoegd, luidende:

Ja

In artikel 161septies vervalt in de aanhef «voor opslag of verwerking van gegevens» en wordt in onderdeel 1° «van de opslag of verwerking» vervangen door: van de opslag, verwerking of overdracht.

11

Artikel I, onderdeel K, subonderdeel 2, komt te luiden:
2. Het tweede lid komt te luiden:
2. Met dezelfde straf wordt gestraft hij die opzettelijk gebruik maakt van de valse of vervalste pas of kaart als ware deze echt en onvervalst, dan wel opzettelijk zodanige pas of kaart aflevert, voorhanden heeft, ontvangt, zich verschaft, vervoert, verkoopt of overdraagt, terwijl hij weet of redelijkerwijs moet vermoeden dat de pas of kaart bestemd is voor zodanig gebruik.

12

Artikel I, onderdeel L, wordt gewijzigd als volgt:

1. De aanhef komt te luiden: Onder vernummering van artikel 273a tot artikel 273f worden na artikel 273 vijf artikelen ingevoegd, luidende:

2. Voor de tekst van artikel 273d wordt de aanduiding «1.» geplaatst en er wordt een lid toegevoegd, luidende:
2. Het eerste lid is van overeenkomstige toepassing op de persoon werkzaam bij een aanbieder van een niet-openbaar telecommunicatie-netwerk of een niet-openbare telecommunicatiedienst.

13

Artikel I, onderdeel N, subonderdeel 1, komt te luiden:
1. In het eerste lid wordt na «geautomatiseerd werk» ingevoegd «of door middel van telecommunicatie».

14

Artikel I, onderdeel O, subonderdeel 1, komt te luiden:
1. In het eerste lid wordt na «geautomatiseerd werk» ingevoegd «of door middel van telecommunicatie».

15

Artikel II, aanhef, komt te luiden:
Indien het bij koninklijke boodschap van 23 februari 2004 ingediende voorstel van wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van de bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens) (29 441) tot wet is of wordt verheven en die wet in werking treedt of is getreden, wordt het Wetboek van Strafvordering als volgt gewijzigd:

16

Artikel II, onderdeel A, komt te luiden:

A

In artikel 67, eerste lid, onderdeel b, wordt na «132,» ingevoegd «138a, 138b, 139c, 139d, eerste en tweede lid, 161sexies, eerste lid, onder 1°, en tweede lid,» en wordt na «350,» ingevoegd: «350a, 351,».

17

Artikel II, onderdeel B, komt te luiden:

B

Aan artikel 125k wordt een lid toegevoegd, luidende:
3. Het bevel, bedoeld in het eerste lid, wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.

17a

Artikel II, onderdeel D, komt te luiden:

D

Artikel 125m, eerste lid, eerste volzin, komt te luiden: Leidt een doorzoeking tot vastlegging of ontoegankelijkmaking van gegevens, dan wordt zo spoedig mogelijk aan de betrokkenen schriftelijk mededeling gedaan van deze vastlegging of ontoegankelijkmaking en van de aard van de vastgelegde of ontoegankelijk gemaakte gegevens.

18

Artikel II, onderdeel E, komt te luiden:

E

Na artikel 125n wordt een artikel ingevoegd, luidende:

Artikel 125o

1. Indien bij een doorzoeking in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten.
2. Onder ontoegankelijkmaking van gegevens wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van het in het eerste lid bedoelde geautomatiseerde werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen van de gegevens uit het geautomatiseerde werk, met behoud van de gegevens ten behoeve van de strafvordering.
3. Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen, bedoeld in het tweede lid, bepaalt de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerde werk worden gesteld.

19

Artikel II, onderdeel G, komt te luiden:

G

Het opschrift van de zevende afdeling van titel IVa van het Eerste Boek komt te luiden «Onderzoek van communicatie door middel van geautomatiseerde werken» en het daarin opgenomen artikel 126m wordt vervangen door drie artikelen, luidende:

Artikel 126la

In deze afdeling wordt verstaan onder:

a. aanbieder van een communicatiedienst: 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;

b. gebruiker van een communicatiedienst: 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.

Artikel 126m

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 onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen.

2. Het bevel is schriftelijk en vermeldt:

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, zijn vervuld;

c. zo mogelijk het nummer of een andere aanduiding waarmee de individuele gebruiker van de communicatiedienst wordt geïdentificeerd alsmede, voor zover bekend, de naam en het adres van de gebruiker;

d. de geldigheidsduur van het bevel;

e. een aanduiding van de aard van het technisch hulpmiddel of de technische hulpmiddelen waarmee de communicatie wordt opgenomen.

3. Indien het bevel betrekking heeft op communicatie die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – het bevel ten uitvoer gelegd met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst en gaat het bevel vergezeld van de vordering van de officier van justitie aan de aanbieder om medewerking te verlenen.

4. Indien het bevel betrekking heeft op andere communicatie dan bedoeld in het derde lid, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel.

5. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging, op vordering van de officier van justitie te

verlenen door de rechter-commissaris. Artikel 126l, vijfde tot en met achtste lid, is van overeenkomstige toepassing.

6. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij of terstond na de toepassing van het eerste lid tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de communicatie, de vordering worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.

7. De in het zesde lid bedoelde vordering wordt niet gericht tot de verdachte.

8. Op de in het zesde lid bedoelde vordering zijn artikel 96a, derde lid, en artikel 126l, vierde, zesde en zevende lid, van overeenkomstige toepassing.

9. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de wijze waarop het in het eerste lid bedoelde bevel en de in het derde en zesde lid bedoelde vorderingen kunnen worden gegeven en over de wijze waarop daaraan wordt voldaan.

Artikel 126ma

1. Indien bij de afgifte van een bevel als bedoeld in artikel 126m, derde lid, bekend is dat de gebruiker van het nummer, bedoeld in artikel 126m, tweede lid, onderdeel c, zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het voornemen tot het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven voordat het bevel ten uitvoer wordt gelegd.

2. Indien na aanvang van het opnemen van de telecommunicatie op grond van het bevel bekend wordt dat de gebruiker zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven.

3. De officier van justitie kan een bevel als bedoeld in artikel 126m, derde lid, eveneens geven, indien het bestaan van het bevel noodzakelijk is om een andere staat te kunnen verzoeken telecommunicatie met een technisch hulpmiddel op te nemen of telecommunicatie af te tappen en rechtstreeks naar Nederland door te geleiden ter fine van opname met een technisch hulpmiddel in Nederland.

20

In artikel II worden na onderdeel G vijf onderdelen ingevoegd, luidende:

Ga

Artikel 126n komt te luiden:

Artikel 126n

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 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.

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.

Gb

Artikel 126na wordt gewijzigd als volgt:

1. In het eerste lid wordt «een gebruiker van telecommunicatie» vervangen door «een gebruiker van een communicatiedienst» en wordt «126n, tweede en derde lid» vervangen door «126n, tweede lid».

2. In het derde lid wordt «126n, vijfde lid» vervangen door «126n, vierde lid».

Gc

In artikel 126nb, eerste lid en derde lid, onderdeel b, wordt «gebruiker van telecommunicatie» telkens vervangen door «gebruiker van een communicatiedienst».

Gd

In artikel 126ng, eerste lid, wordt «de aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk de aanbieder van een openbare telecommunicatiedienst» vervangen door: de aanbieder van een communicatiedienst in de zin van artikel 126la».

Ge

Na artikel 126nh wordt een artikel ingevoegd, luidende:

Artikel 126ni

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 126la 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.

21

Artikel II, onderdeel I, komt te luiden:

I

Artikel 126t komt te luiden:

Artikel 126t

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst in de zin van artikel 126la, wordt opgenomen.

2. Het bevel is schriftelijk en vermeldt:

a. een omschrijving van het georganiseerd verband;

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

c. zo mogelijk het nummer waarmee de individuele gebruiker van de

communicatiedienst wordt geïdentificeerd alsmede, voor zover bekend, de naam en het adres van de gebruiker;

d. de naam van de persoon, genoemd in het eerste lid, wanneer deze niet de houder is;

e. de geldigheidsduur van het bevel; en

f. een aanduiding van de aard van het technisch hulpmiddel of de technische hulpmiddelen waarmee de communicatie wordt opgenomen.

3. Indien het bevel betrekking heeft op communicatie die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – het bevel ten uitvoer gelegd met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst en gaat het bevel vergezeld van een vordering aan de aanbieder om medewerking te verlenen.

4. Indien het bevel betrekking heeft op andere communicatie dan bedoeld in het derde lid, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel.

5. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 126s, vijfde tot en met achtste lid, is van overeenkomstige toepassing.

6. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij of terstond na de toepassing van het eerste lid tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de communicatie, de vordering worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.

7. De in het zesde lid bedoelde vordering wordt niet gericht tot de verdachte.

8. Op de in het zesde lid bedoelde vordering zijn artikel 96a, derde lid, en artikel 126s, vierde, zesde en zevende lid, van overeenkomstige toepassing.

9. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de wijze waarop het in het eerste lid bedoelde bevel en de in het derde en zesde lid bedoelde vorderingen worden gegeven en over de wijze waarop daaraan wordt voldaan.

22

In artikel II worden na onderdeel I acht onderdelen ingevoegd, luidende:

Ia

Na artikel 126t wordt een artikel ingevoegd, luidende:

Artikel 126ta

1. Indien bij de afgifte van een bevel als bedoeld in artikel 126t, derde lid, bekend is dat de gebruiker van het nummer, bedoeld in artikel 126t, tweede lid, onderdeel c, zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het voornemen tot het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven voordat het bevel ten uitvoer wordt gelegd.

2. De officier van justitie kan een bevel als bedoeld in artikel 126t, derde lid, eveneens geven, indien het bestaan van het bevel noodzakelijk is om een andere staat te kunnen verzoeken telecommunicatie met een

technisch hulpmiddel op te nemen of telecommunicatie af te tappen en rechtstreeks naar Nederland door te geleiden ter fine van opname met een technisch hulpmiddel in Nederland.

Ib

Artikel 126u komt te luiden:

Artikel 126u

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 126la 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.
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.

Ic

Artikel 126ua wordt gewijzigd als volgt:

1. In het eerste lid wordt «telecommunicatie» vervangen door «een communicatiedienst in de zin van artikel 126la» en wordt «Artikel 126u, tweede en derde lid» vervangen door «Artikel 126u, tweede lid».

2. In het derde lid wordt «artikel 126u, vijfde lid» vervangen door «artikel 126u, vierde lid».

Id

In artikel 126ub wordt «een gebruiker van telecommunicatie» vervangen door «een gebruiker van een communicatiedienst» en wordt «126na» vervangen door «126nb».

Ie

In artikel 126ug, eerste lid, wordt na «een openbaar» ingevoegd «of een niet-openbaar» en wordt na «een openbare» ingevoegd «of een niet-openbare».

If

Na artikel 126uh wordt een artikel ingevoegd, luidende:

Artikel 126ui

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.

Ig

In artikel 126bb, vijfde lid, wordt «126nh» vervangen door «126ni» en «126uh» door «126ui».

Ih

In artikel 126ee, onderdeel a, wordt «de artikelen 126g, derde lid, 126l, eerste lid, 126o, derde lid, en 126s, eerste lid;» vervangen door «de artikelen 126g, derde lid, 126l, eerste lid, 126m, eerste lid, 126o, derde lid, 126s, eerste lid, en 126t, eerste lid;».

23

In artikel II, onderdeel K, komt het eerste lid van artikel 552a te luiden:
1. De belanghebbenden kunnen zich schriftelijk beklagen over inbeslagneming, over het gebruik van in beslag genomen voorwerpen, over het uitblijven van een last tot teruggave, over de vordering van gegevens, over de vordering medewerking te verlenen aan het ontsleutelen van gegevens, over de kennisneming of het gebruik van gegevens, vastgelegd tijdens een doorzoeking of op vordering verstrekt, over de kennisneming of het gebruik van gegevens, opgeslagen, verwerkt of overgedragen door middel van een geautomatiseerd werk en vastgelegd bij een onderzoek in zodanig werk, over de kennisneming of het gebruik van gegevens als bedoeld in de artikelen 100, 101 en 114, over de vordering gegevens te bewaren en beschikbaar te houden, alsmede over de ontoegankelijkmaking van gegevens, aangetroffen in een geautomatiseerd werk, bedoeld in artikel 125o, de opheffing van de desbetreffende maatregelen of het uitblijven van een last tot zodanige opheffing.

24

In artikel II wordt na onderdeel L een onderdeel toegevoegd, luidende:

M

In artikel 592, tweede lid, wordt «126nc tot en met 126nh en 126uc tot en met 126uh» vervangen door: 126m, 126n, 126nc tot en met 126ni, 126t, 126u, 126uc tot en met 126ui.

25

Na artikel II wordt een artikel ingevoegd, luidende:

ARTIKEL IIA

Aan artikel 51a, tweede lid, van de Uitleveringswet wordt, onder vervanging van de punt aan het slot door een puntkomma, een onderdeel toegevoegd, luidende:

– de misdrijven, strafbaar gesteld in de artikelen 138a, 138b, 139c, 139d, 161sexies, 225, 226, 227, 240a, 240b, 326, 326c, 350, 350a en 351 van het Wetboek van Strafrecht, de artikelen 31a en 31b van de Auteurswet 1912 en de artikelen 22 en 23 van de Wet op de naburige rechten, voor zover het feit valt onder de omschrijving van de artikelen 2 tot en met 10 van het op 23 november 2001 te Budapest tot stand gekomen Internationaal Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18).

26

In artikel III komt onderdeel A te luiden:

A

In artikel 13.2b wordt «126nh» vervangen door «126ni» en «126uh» door «126ui».

27

In artikel IV vervallen het eerste en tweede lid alsmede de aanduiding «3.» voor het derde lid.

28

Na artikel IV worden twee artikelen ingevoegd, luidende:

ARTIKEL IVA

Artikel II van de wet van 21 april 2004 tot wijziging van het Wetboek van Strafrecht in verband met de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (fraude niet-chartaal geldverkeer) (Stb. 180) vervalt.

ARTIKEL IVB

Indien het bij koninklijke boodschap van 23 februari 2004 ingediende voorstel van wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens (29 441) tot wet is of wordt verheven, vervallen de artikelen IV en V van die wet.

TOELICHTING

1. Algemeen

1.1. Inleiding

Met deze nota van wijziging wordt het onderhavige wetsvoorstel op drie punten gewijzigd.

– Ten eerste wordt het wetsvoorstel uitgebreid met een aantal wetswijzigingen die nodig zijn om het op 23 november 2001 tot stand gekomen «Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken» (Trb 2002, nr. 18, hierna aangeduid als «het Verdrag» of, naar zijn Engelse titel, als «het Cybercrime Verdrag») te kunnen ratificeren. Het betreft vooral wijzigingen in het Wetboek van Strafrecht en het Wetboek van Strafvordering. Op dit onderdeel bestaat een nauwe samenhang met het gelijktijdig met deze nota van wijziging ingediende voorstel van wet tot goedkeuring van het Cybercrime Verdrag (Kamerstukken II 2004/05, ...).

– Ten tweede worden enkele – vooral strafvorderlijke – wijzigingen uit het wetsvoorstel verwijderd, omdat het daarbij gaat om onderwerpen die inmiddels in een breder verband zijn opgenomen in het bij de Tweede Kamer aanhangige voorstel van wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens) (29 441).

– Ten slotte wordt het wetsvoorstel aangepast aan een aantal inmiddels in werking getreden of aanhangige wetswijzigingen.

De voortgang van de schriftelijke behandeling van het onderhavige wetsvoorstel heeft geruime tijd stilgelegen in verband met de samenloop van dit wetsvoorstel met andere ontwikkelingen. Een cruciaal onderdeel van het wetsvoorstel betrof de regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen. Juist ten aanzien van dit onderdeel constateerde de Europese Commissie dat de regeling onverenigbaar was met het stelsel van aansprakelijkheid zoals neergelegd in de (toen nog: ontwerp-) richtlijn inzake e-commerce. Daarom is de bedoelde regeling bij nota van wijziging uit het wetsvoorstel verwijderd. Inmiddels is een nieuwe regeling van de strafrechtelijke aansprakelijkheid van de tussenpersoon door middel van de Aanpassingswet richtlijn inzake elektronische handel (Stb. 2004, 210) opgenomen in het nieuwe artikel 54a in het Wetboek van Strafrecht.

Het wetsvoorstel dient op onderdelen te worden aangepast aan het Cybercrime Verdrag. Voor de implementatie van het Verdrag is immers wijziging nodig van onder meer het Wetboek van Strafrecht (Sr) en het Wetboek van Strafvordering (Sv), op onderdelen die ook door het wetsvoorstel computercriminaliteit II worden bestreken.

Voor een deel zijn de voor implementatie van het Verdrag benodigde wijzigingen reeds langs andere weg tot stand gekomen. Wat betreft het materieelrechtelijke deel vond bijvoorbeeld, vooruitlopend op de totstandkoming van het Verdrag, in het kader van de herziening van de zedelijkheidswetgeving reeds wijziging plaats van artikel 240b Sr (Stb. 2002, 388). Door deze wijziging voldoet onze wetgeving aan artikel 9 van het Verdrag. Wat betreft het strafvorderlijke deel kent het Wetboek van Strafvordering inmiddels bevoegdheden tot het vorderen van gegevens van bedrijven in de openbare telecommunicatiesector en in de financiële sector, waardoor terzake van die sectoren wordt voldaan aan enkele bepalingen van het Verdrag. Het Verdrag heeft evenwel een wijdere strekking, zodat nadere aanpassing nodig is. Inmiddels is bij de Tweede Kamer ook aanhangig het eerder genoemde wetsvoorstel inzake

bevoegdheden vorderen gegevens (Kamerstukken II 2003–04, 29 441). Daarbij worden algemene bevoegdheden in het leven geroepen tot het vorderen van gegevens, waarbij in beginsel irrelevant is over wat voor soort gegevens het gaat en op wat voor gegevensdrager zij eventueel vastliggen. Die bevoegdheden voorzien voor een deel in algemene zin in de materie die in het Verdrag specifiek voor computergegevens is geregeld. In de hierna volgende hoofdstukken wordt hierop nader ingegaan.

1.2. Aparte wijzigingswet of onderbrenging in wetsvoorstel Computercriminaliteit II?

Bij brieven van 23 december 1999 (Kamerstukken II 1999/2000, 23 530, nr. 40) en van 27 november 2000 (Kamerstukken II 2000/2001, 23 530, nr. 45) is de Tweede Kamer ingelicht over de voortgang van het Cybercrime Verdrag en over de relatie met de Nederlandse wetgeving. Daarbij heeft de regering reeds aangegeven voorstander te zijn van ratificatie van het Cybercrime Verdrag. Daartoe strekt het eerder genoemde voorstel voor een goedkeuringswet.

De vraag deed zich voor of de voor implementatie nog noodzakelijke wetswijzigingen zouden moeten worden opgenomen in een apart wetsvoorstel of dat zou moeten worden aangesloten bij het aanhangige wetsvoorstel computercriminaliteit II. Ik heb voor deze laatste optie gekozen om het reeds aanzienlijke aantal wetten en wetsvoorstellen waarin wijziging wordt aangebracht in de strafvorderlijke bevoegdheden terzake van het verkrijgen van (computer- en andere) gegevens niet nog verder te vergroten. Weliswaar was denkbaar geweest om het wetsvoorstel computercriminaliteit II in te trekken, maar dan had een aantal van de daarin voorkomende wetswijzigingen toch weer opgenomen moeten worden in het nieuw in te dienen wetsvoorstel. Daarbij komt dat de Tweede Kamer in november 2000 een verslag heeft uitgebracht, dat nog beantwoording behoeft. Alles afwegende heb ik ervoor gekozen de voor het Cybercrime Verdrag nog noodzakelijke wetswijzigingen door middel van één nota van wijziging (waarbij ook wijzigingen van andere aard worden meegenomen) in te brengen in het wetsvoorstel computercriminaliteit II. Gelet op het belang en het karakter van de wijzigingen lag het wel voor de hand de nota van wijziging ter advisering voor te leggen aan de Raad van State. Voorafgaand daaraan is aan een aantal instanties advies gevraagd over specifiek die wijzigingen die voortvloeien uit het Cybercrime Verdrag.

Zoals in de inleiding gemeld, betreft de bijgaande nota van wijziging ook wijzigingen van meer technische aard, onder meer ter aanpassing van het wetsvoorstel aan inmiddels tot stand gekomen en aanhangige wetgeving. Naar aanleiding van de beantwoording van het verslag van de Tweede Kamer zullen wellicht ook nog enige wijzigingen moeten worden aangebracht. Deze wijzigingen zullen alsdan plaatskrijgen in een aparte nota van wijziging, die aan de Tweede Kamer zal worden aangeboden gelijktijdig met de beantwoording van het verslag.

1.3. Opbouw van deze toelichting

Voordat ik de onderdelen van de nota van wijziging in hoofdstuk 3 artikelsgewijs toelicht, zal ik in hoofdstuk 2 van deze toelichting kort ingaan op de inhoud en de totstandkoming van het Cybercrime Verdrag; voor een uitvoeriger toelichting zij verwezen naar de memorie van toelichting bij het voorstel voor de goedkeuringswet. In deze toelichting zal ik wel uitvoerig ingaan op de vraag in hoeverre Nederland al voldoet aan de verplichtingen die op de verdragsluitende partijen rusten. Waar nodig wordt daarbij aangegeven tot welke wetswijzingen het Cybercrime Verdrag aanleiding geeft. In dat hoofdstuk ga ik ook kort in op de

verhouding tussen het onderhavige wetsvoorstel en andere relevante wetsvoorstellen, waaronder het hierboven genoemde wetsvoorstel inzake bevoegdheden vorderen gegevens.

Hoofdstuk 3 tenslotte bevat de toelichting op de onderdelen van de nota van wijziging.

2. Het Cybercrime Verdrag en de toepasselijke Nederlandse wetgeving

2.1. Korte weergave van de inhoud van het Verdrag

Het Verdrag strekt kortgezegd tot een gemeenschappelijk strafrechtelijk beleid, gericht op de bescherming van de samenleving tegen strafbare feiten verbonden met elektronische netwerken, vooral door het tot stand brengen van passende wetgeving en het versterken van de internationale samenwerking. De afgelopen decennia zijn ingrijpende veranderingen teweeggebracht door de digitalisering en door de voortschrijdende mondialisering van computernetwerken, waardoor het risico is toegenomen dat computernetwerken en elektronische informatie worden gebruikt voor het begaan van strafbare feiten terwijl tegelijkertijd eventuele bewijzen met betrekking tot strafbare feiten door deze netwerken kunnen worden opgeslagen en overgedragen. Voor een doeltreffende bestrijding van strafbare feiten verbonden met elektronische netwerken is een snelle en adequate internationale samenwerking noodzakelijk.

Het Verdrag treedt in werking als minimaal vijf staten, waaronder minimaal drie lidstaten van de Raad van Europa, het Verdrag hebben geratificeerd. Aan deze voorwaarde is inmiddels voldaan; het Verdrag is met ingang van 1 juli 2004 in werking getreden. Verreweg de meeste staten die het Verdrag hebben ondertekend, zijn evenwel nog niet tot ratificatie overgegaan. De verwachting is dat dit in 2005 voor een groot aantal landen wel het geval zal zijn. Zoals aangegeven is inmiddels, synchroon met de onderhavige nota van wijziging, het voorstel voor de goedkeuringswet in procedure gebracht.

Het Verdrag kent vier soorten bepalingen: bepalingen van materieel strafrechtelijke aard, bepalingen van strafvorderlijke aard, bepalingen inzake internationale samenwerking en tenslotte inwerkingtredings- en overige bepalingen.

Het materieel-strafrechtelijke deel omschrijft een aantal gedragingen die de landen in hun nationale wetgeving strafbaar dienen te stellen. Het gaat – kort weergegeven – om wederrechtelijke toegang tot computersystemen (artikel 2 van het Verdrag), wederrechtelijke onderschepping van computergegevens (artikel 3), verstoring van computergegevens (artikel 4), verstoring van computersystemen (artikel 5), een aantal voorbereidingshandelingen voor de feiten bedoeld in de artikelen 2 t/m 5 (artikel 6), vervalsing van computergegevens (artikel 7), computergerelateerde fraude (artikel 8), inhoudgerelateerde misdrijven (misdrijven in verband met kinderpornografie, artikel 9) en auteursrechtelijke misdrijven (artikel 10).

Het strafvorderlijke deel omschrijft een aantal bevoegdheden die de landen in hun nationale wetgeving dienen toe te kennen aan de met opsporing van strafbare feiten belaste organen. In het kort weergegeven gaat het om de tijdelijke «bevriezing» van bepaalde opgeslagen maar vluchtige gegevens (artikel 16), de tijdelijke «bevriezing» en eventuele ontsluiting van verkeersgegevens (artikel 17), een bevel om specifieke computergegevens waaronder abonneegegevens te verstrekken (artikel

18), de bevoegdheid om computers en computergegevens te doorzoeken en eventueel in beslag te nemen c.q. te kopiëren (artikel 19), de verstrekking van verkeersgegevens (artikel 20) en de onderschepping van specifieke inhoudgegevens (artikel 21).

Voor een nadere aanduiding van de inhoud van het Cybercrime Verdrag verwijs ik naar de memorie van toelichting bij het Voorstel van wet houdende goedkeuring van het Verdrag (vindplaats PM).

2.2. Uitgebrachte adviezen

De voorstellen die zijn opgenomen in de nota van wijziging en die betrekking hebben op de implementatie van het Cybercrime Verdrag, zijn ter consultatie voorgelegd aan de Nederlandse Orde van Advocaten (NovA), de Nederlandse Vereniging voor Rechtspraak (NVvR), de Raad voor de Rechtspraak, het openbaar ministerie (OM), het College bescherming persoonsgegevens (CBP), het Overlegplatform Post en Telecommunicatie (OPT) en het VNO-NCW. Commentaar is ontvangen van de NOVA, de NVVR, het OM, het OPT en het CBP[1]. De Raad voor de Rechtspraak (RvdR) heeft zich aangesloten bij het advies van het OM.

Algemeen

Tot mijn genoegen zijn de adviezen positief over het voornemen om tot ratificatie van het Verdrag over te gaan. De adviesinstanties stemmen, met uitzondering van het CBP, in grote lijnen ook in met de wijze van implementatie en met de daarbij gemaakte keuzes.

In enkele adviezen, nl. van de NVVR, het OM en het CBP, wordt zorg uitgesproken over de onoverzichtelijkheid van het wettelijk stelsel door de opeenstapeling van wetswijzigingen, vooral op strafvorderlijk terrein. Dit is ook voor mij een belangrijk punt van aandacht. Hoewel niet te vermijden is dat diverse wetswijzigingen elkaar opvolgen, kan en wil ik er wel zoveel mogelijk aan bijdragen dat het overzicht bewaard blijft. Daarom heb ik niet alleen in de toelichting hieronder een opsomming gegeven van de wettelijke bepalingen die voor het onderhavige voorstel relevant zijn, maar heb ik ook een bijlage bij deze nota van wijziging gevoegd waarin een doorlopende tekst is opgenomen van de relevante onderdelen van het Wetboek van Strafvordering, en wel naar de tekst zoals de artikelen luiden na verwerking van alle inmiddels tot stand gekomen wetswijzigingen c.q. zoals de artikelen zullen luiden na verwerking van de nog aanhangige (andere) wetsvoorstellen, maar vóór verwerking van de in deze nota van wijziging voorgestelde teksten. Dit overzicht is primair bedoeld voor een goede beoordeling van de thans voorgestelde wetswijzigingen maar kan ook daarnaast een nuttig inzicht bieden in de wijzigingen van deze artikelen.

De door de adviseurs gewenste overzichtelijkheid van het stelsel heeft mij er ook toe geleid de regeling voor het opnemen van communicatie bij de niet-openbare netwerken in die zin te vereenvoudigen, dat deze wordt samengenomen met de regeling die thans bestaat voor het opnemen van telecommunicatie bij de openbare netwerken.

Adviezen van NVVR, NOVA, OM, RvdR en OPT

Zowel de NVVR als het OM (en daarmee tevens de RvdR) hebben geadviseerd de in het voorontwerp opgenomen wijziging van artikel 126m Sv te heroverwegen en anders op te zetten. Dit advies heb ik overgenomen. Op de nieuwe opzet van artikel 126m Sv (en het daarmee corresponderende artikel 126t Sv) wordt in deze toelichting nader ingegaan.

De NOVA heeft geadviseerd in de toelichting in te gaan op de bescherming van de grondrechten van de burger, in het licht van artikel 15

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

van het Verdrag. Ook dit advies heb ik overgenomen; ik verwijs naar paragraaf 3.1 hierna.

Het OPT heeft gevraagd om in de toelichting uitdrukkelijk in te gaan op de gevolgen van de introductie van de zgn. bevriezingsbevoegdheid (artikel 16 van het Verdrag) voor mobiele telecomoperators. Ook hieraan heb ik gevolg gegeven, en wel in de toelichting op het voorgestelde artikel 126ni Sv.

Het OM is in zijn advies, naar aanleiding van het voorstel om artikel 67 Sv aan te vullen met de vermelding van specifieke computerdelicten, ingegaan op de verhouding tussen dwangmiddelen en de zwaarte van de strafdreiging bij de delicten voor de opsporing waarvan die dwangmiddelen kunnen worden toegepast. Het OM constateert dat bij een aantal van de computerdelicten die aan artikel 67 worden toegevoegd, voorlopige hechtenis weliswaar een adequate reactie is, maar vraagt zich af of de voorgestelde strafdreiging bij die computerdelicten dan wel in overeenstemming is met de ernst van de omschreven feiten. Hiermee lijkt het OM eraan voorbij te gaan dat artikel 67 een tweedeling kent in de systematiek. In algemene zin wordt in onderdeel a van artikel 67, eerste lid, voorlopige hechtenis mogelijk gemaakt voor alle delicten waarop een gevangenisstraf van vier jaar of meer is gesteld; daarbij is de strafmaat inderdaad relevant. Maar daarnaast is in de onderdelen b (voor zover het betreft het Wetboek van Strafrecht) en c (voor zover het andere wetten betreft) een aanzienlijke lijst van delicten opgenomen waarbij voorlopige hechtenis mogelijk wordt gemaakt – en ook andere strafvorderlijke bevoegdheden toegepast kunnen worden – omdat de *aard* van de strafbare gedragingen daartoe aanleiding geeft, maar waarbij de bedreiging van straf lager is dan vier jaar. Niettemin heeft het advies van het OM mij wel aanleiding gegeven de strafmaat van de specifieke computerdelicten nog eens te bezien. In een aantal gevallen moet geconstateerd worden dat de destijds opgenomen strafmaat niet meer als adequaat kan worden beschouwd. In het bijzonder de op computervredebreuk (artikel 138a Sr) gestelde maximumstraf van 6 maanden gevangenisstraf acht ik niet meer adequaat, in het licht van de grote maatschappelijke schade die daarvan het gevolg kan zijn. Ik stel voor de hierop gestelde maximumstraf te verhogen tot een jaar, evenals bij enkele andere computerdelicten waarop thans nog een maximumstraf van 6 maanden is gesteld.

Het advies van het CBP

Het CBP bepleit in zijn advies een verruiming van de reikwijdte van de strafbaarstelling van de schending van het telefoongeheim tot de niet-openbare telecommunicatiediensten ennetwerken. Het CBP merkt daarbij op dat inbreuken op communicatie middels niet-openbare netwerken veelal niet strafbaar zijn indien deze worden gepleegd door de rechthebbende op het netwerk. De door het CBP aan de orde gestelde vraag of niet ook aan de toegang van de rechthebbende tot communicatie over zijn eigen netwerk nadere voorwaarden dienen te worden gesteld ter bescherming van het telecommunicatiegeheim van de gebruikers van dat netwerk, beantwoord ik bevestigend. Zeker voor omvangrijke private netwerken waarin vele duizenden personen plegen te communiceren in verschillende posities en onderlinge verhoudingen en met uiteenlopende redelijke verwachtingen ten aanzien van de bescherming van de vertrouwelijkheid van de communicatie, acht ook ik nadere voorwaarden wenselijk. Daarom stel ik voor de reikwijdte van artikel 273d Sr – dat overeenkomstig het onderhavige wetsvoorstel in de plaats treedt van het huidige artikel 374bis waarnaar het CBP verwijst – te verruimen naar de niet-openbare telecommunicatienetwerken en -diensten. Het opzettelijk en wederrechtelijk kennisnemen, overnemen, aftappen of opnemen van gegevens die door tussenkomst van zodanige netwerken of diensten worden verwerkt of overgedragen en die niet voor betrokkene bestemd

zijn, wordt hiermee strafbaar. Onder welke omstandigheden sprake zal zijn van wederrechtelijk handelen van de rechthebbende – veelal de werkgever – en in welke gevallen de gegevens al of niet mede bestemd moeten worden geacht voor die rechthebbende, zal afhangen van de feitelijke beoordeling van de situatie, waarbij een grote betekenis zal moeten worden toegekend aan de afspraken die over het gebruik van de diensten en netwerken worden gemaakt. Teneinde een zorgvuldige invoering van deze uitbreiding van de strafbepaling mogelijk te maken, is het wenselijk de inwerkingtreding te kunnen laten plaatsvinden op een later tijdstip dan de andere delen van het wetsvoorstel. Met het oog daarop is deze uitbreiding vormgegeven in een apart tweede lid bij het voorgestelde artikel 273d Sr.

Het CBP neemt in zijn advies als standpunt in, dat het Cybercrime Verdrag moet worden beschouwd als een maatgevend voorstel waar het gaat om het opsporen van criminele gedragingen waarbij computernetwerken worden gebruikt alsmede het vergaren van elektronisch bewijsmateriaal. Het CBP verbindt daaraan de – voor zijn verdere advies cruciale – conclusie dat de al bestaande wettelijke bepalingen aan het Verdrag dienen te worden getoetst. De in bedoelde paragraaf opgenomen beschouwingen van het CBP gaan evenwel uit van een opvatting over het Cybercrime Verdrag die naar mijn stellige overtuiging niet overeenkomt met de betekenis die de Verdragsluitende partijen daaraan hebben toegekend. In het Verdrag zijn die punten vastgelegd, waarover de verdragsluitende partijen overeenstemming hebben bereikt. Het Verdrag heeft niet de pretentie – en kan die pretentie ook niet hebben – om de daarin opgenomen onderwerpen uitputtend te regelen. Het Verdrag heeft, zoals de meeste internationale regelingen, dan ook een minimumkarakter. De individuele verdragspartijen zijn bevoegd tot het treffen of instandhouden van maatregelen die niet in het Verdrag zijn overeengekomen, mits deze geen strijd opleveren met het in het Verdrag bepaalde. Dit uitgangspunt is, voor zover nog nodig, ook uitdrukkelijk vastgelegd in artikel 39, derde lid, van het Verdrag. Weliswaar wijst ook het CBP daarop, maar hij ontleent aan artikel 15 van het Verdrag argumenten voor de stelling dat niet kan worden volstaan met toevoeging van vanwege het Cybercrime Verdrag vereiste bevoegdheden. Het nieuw te creëren stelsel van bevoegdheden dient naar de opvatting van het CBP tevens een opschoning van het bestaande arsenaal aan opsporingsmiddelen met zich te brengen. Hiermee wordt evenwel een uitleg gegeven aan artikel 15 van het Verdrag die niet overeenstemt met de bedoeling daarvan. Artikel 15 is niet bedoeld – en kan ook niet bedoeld zijn – als een opdracht aan partijen om bestaande bevoegdheden op te schonen. Artikel 15 richt zich op de wijze waarop de individuele maatregelen van toepassingsvoorwaarden en waarborgen kunnen worden voorzien. Gezien de samenhang en de structuur van het bestaande nationale recht kan het Verdrag niet verder gaan dan dit algemeen gestelde voorschrift. Het is aan de nationale wetgever overgelaten op welke wijze hij daaraan vorm en inhoud geeft. Dat de nationale wetgever bij het tot stand brengen van nieuwe bevoegdheden rekening dient te houden met reeds bestaande bevoegdheden en dat dit van invloed kan zijn op de wijze waarop de verdragstekst wordt geïmplementeerd, is evident. In de toelichting op deze nota van wijziging wordt daarop dan ook uitvoerig ingegaan. Dit geldt overigens niet alleen voor de verhouding tussen de verschillende strafvorderlijke bevoegdheden maar ook voor de verhouding tussen de diverse strafbepalingen.

Het CBP is ook op enkele andere punten kritisch over de voorgestelde wijze van implementeren. Zo stelt het CBP aan het slot van paragraaf 3 van zijn advies onder meer dat door de voorgestelde wijze van implementeren de vorderingsbevoegdheden van het Verdrag toepasbaar worden ter opsporing van andere delicten dan bedoeld in het Verdrag, wat naar de

opvatting van het CBP een «bovenmatige vorm van meeliften met het Cybercrime Verdrag» is, die ten minste afzonderlijk in de toelichting dient te worden verantwoord. Het CBP lijkt hiermee te miskennen dat artikel 14 van het Verdrag uitdrukkelijk aan de verdragspartijen voorschrijft ervoor te zorgen dat de bevoegdheden kunnen worden toegepast niet alleen ten aanzien van (a) de feiten, bedoeld in de artikelen 2 tot en met 11 van het Verdrag, maar ook ten aanzien van (b) andere door middel van een computersysteem begane strafbare feiten en bovendien voor (c) de vergaring van bewijs in elektronische vorm van *enig strafbaar feit*. In de praktijk komt dit neer op alle delicten voor de opsporing waarvan elektronisch bewijs moet worden vergaard. In de toelichting wordt hierop ingegaan.

Het CBP heeft aandacht gevraagd voor de mogelijke samenloop van bestaande en nieuwe bevoegdheden. Mede naar aanleiding van dit advies zijn in de bijgaande voorstellen enkele voorzieningen getroffen voor een betere afgrenzing van bevoegdheden. Het advies van het CBP heeft mij tenslotte aanleiding gegeven de nieuwe bevoegdheden nog eens kritisch te bezien. Dat heeft er onder meer toe geleid dat thans wordt voorgesteld de zogenaamde bevriezingsbevoegdheid (in het nieuwe artikel 126ni Sv) slechts mogelijk te maken 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, en de bevoegdheid niet bij de hulpofficier maar bij de officier van justitie te leggen.

2.3. Relevante Nederlandse wetgeving

Voor een groot deel voldoet Nederland nu al aan hetgeen waartoe het Verdrag verplicht.

a. Wat betreft het materiële strafrecht is van belang dat het Wetboek van Strafrecht in de negentiger jaren van de vorige eeuw is uitgebreid met bepalingen die specifiek zijn toegespitst op strafbare feiten door middel van of met betrekking tot geautomatiseerde werken (de Wet computercriminaliteit, Stb. 1993, 33). Het onderhavige wetsvoorstel «computercriminaliteit II» is daarop een vervolg. Voor het materieel-strafrechtelijke deel van het Verdrag zijn voor de Nederlandse situatie ten eerste relevant een aantal specifiek op geautomatiseerde werken c.q. telecommunicatie gerichte artikelen in het Wetboek van Strafrecht. Het betreft de artikelen 138a (computervredebreuk), 139a t/m 139d (voor zover betrekking hebbend op het aftappen en opnemen van computergegevens), 161sexies en 161septies (vernieling etc. van geautomatiseerde werken en werken voor telecommunicatie), 326c (listiglijk gebruik maken van telecommunicatiediensten), 350a en 350b (beschadiging van computergegevens) en 351 en 351bis (voor zover betrekking hebbend op de beschadiging van geautomatiseerde werken ten algemenen nutte). Naar Nederlands recht valt een aantal volgens het Verdrag strafbaar te stellen gedragingen ook binnen de termen van commune delicten, zoals valsheid in geschrift (artikelen 225 en 226 Sr) en vernieling (artikel 350 Sr).

b. Wat betreft het strafvorderlijk deel is van belang dat de «gewone» strafvorderlijke bepalingen al in belangrijke mate tegemoet komen aan de eisen van het Verdrag. Daarnaast zijn de nodige wetgevende initiatieven genomen om het Wetboek van Strafvordering uit te breiden met bepalingen die gericht zijn hetzij op het vorderen van gegevens in het algemeen hetzij op het vorderen van gegevens in het kader van telecommunicatie. Naast het onderhavige wetsvoorstel computercriminaliteit II kunnen in het bijzonder genoemd worden de wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in

verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens inzake telecommunicatie (vorderen gegevens telecommunicatie) (Stb. 105) en het voorstel van wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens) (29 441).

Van het Wetboek van Strafvordering is ten eerste van belang de Zevende Afdeling van Titel IV van boek I, welke afdeling is ingevoegd bij de Wet computercriminaliteit (Stb. 1993, 33). Het betreft de artikelen 125i t/m 125n. Wijziging en aanvulling van deze artikelen wordt voorzien in het onderhavige wetsvoorstel computercriminaliteit II (26 671) en in het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441).

Vervolgens is van belang een aantal bepalingen, opgenomen in Titel IVa (Bijzondere bevoegdheden tot opsporing). Het gaat daarbij in het bijzonder om de Zesde, Zevende en Achtste Afdeling, zoals gewijzigd en aangevuld in een aantal aanhangige en in voorbereiding zijnde wetsvoorstellen. De Zesde Afdeling bestaat uit artikel 126l, dat de bevoegdheid van opsporingsambtenaren betreft om vertrouwelijke communicatie met een technisch hulpmiddel op te nemen. De Zevende Afdeling (Onderzoek van telecommunicatie) bevat de volgende artikelen:- artikel 126m, betreffende de bevoegdheid om, mede op grond van artikel 13.2 van de Telecommunicatiewet, van telecommunicatiebedrijven de medewerking te vorderen bij het met een technisch hulpmiddel opnemen van telecommunicatie; het artikel is op een specifiek onderdeel aangevuld door middel van de Uitvoeringswet EU-rechtshulpovereenkomst (Stb. 2004, 107) en wordt bovendien aangevuld in het onderhavige wetsvoorstel computercriminaliteit II;

– artikel 126n, betrekking hebbend op het vorderen van verkeersgegevens bij telecombedrijven; de bepaling is gewijzigd bij de wet van 18 maart 2004 (Stb. 105) (vorderen gegevens telecommunicatie);

– artikel 126na (nieuw), betrekking hebbend op het vorderen van de zogenaamde «NAW-gegevens» (naam, adres etc.) bij telecombedrijven; het artikel is ingevoegd bij de Wet van 18 maart 2004 (Stb. 105) (vorderen gegevens telecommunicatie);

– artikel 126nb (voor de inwerkingtreding van de Wet van 18 maart 2004 (Stb. 105) aangeduid als artikel 126na), betrekking hebbend op het verkrijgen van het nummer, teneinde toepassing te kunnen geven aan de artikelen 126m en 126n. De Achtste Afdeling betreft het Vorderen van gegevens in de financiële sector (ingevoegd bij de Wet van 18 maart 2004 (Stb. 109) (Vorderen gegevens financiële sector), maar deze zal qua reikwijdte ingrijpend worden uitgebreid door middel van het wetsvoorstel inake bevoegdheden vorderen gegevens (29 441).

Ten slotte is nog van belang Titel V van het Wetboek van Strafvordering, betreffende bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband. In deze titel wordt een aantal strafvorderlijke bevoegdheden voor de hier bedoelde situatie geregeld die gelijk zijn aan de bevoegdheden in titel IVa. Voor het onderhavige terrein zijn in het bijzonder van belang de artikelen 126q (wijziging aanhangig door het onderhavige wetsvoorstel computercriminaliteit II), 126t (idem, tevens inmiddels gewijzigd door de wet van 18 maart 2004 (Stb. 107) (Uitvoeringswet EU-rechtshulpovereenkomst), 126u t/m 126ub (gewijzigd door de wet inzake vorderen gegevens telecom), en een aantal bepalingen die zullen worden toegevoegd door het wetsvoorstel inzake bevoegdheden vorderen gegevens.

In het vorenstaande komt duidelijk naar voren dat sommige strafvorderlijke onderwerpen in verschillende wetgevingstrajecten een rol spelen. Dat doet zich vooral voor bij onderwerpen die zowel in het wetsvoorstel computercriminaliteit II aan de orde komen als in het wetsvoorstel inzake bevoegdheden vorderen gegevens. Een aantal wetswijzigingen, voorgesteld bij het wetsvoorstel computercriminaliteit II, kan vervallen nu dat andere wetsvoorstel is ingediend. Dit zal in technische zin zijn beslag krijgen door middel van een nota van wijziging bij het onderhavige wetsvoorstel computercriminaliteit II en, indien nodig, door middel van wijzigingsbepalingen in het andere wetsvoorstel.

Vooral de zevende en achtste afdeling van titel IVa van het Wetboek van Strafvordering zijn onderwerp van diverse recent tot stand gekomen en in behandeling zijnde wetswijzigingen. Ten behoeve van de lezer is daarom in bijlage II een doorlopende tekst opgenomen van deze afdelingen, zoals deze zouden komen te luiden na verwerking van de daarbij vermelde wetswijzigingen, maar zonder verwerking van het onderhavige wetsvoorstel computercriminaliteit II.

c. De bepalingen inzake internationale samenwerking zijn deels van feitelijke aard, waar bepaalde informatieverplichtingen en andere handelwijzen worden voorgeschreven. Deels hangen de bepalingen nauw samen met de bepalingen van strafvorderlijke aard, waar staten dienen samen te werken bij het verkrijgen van computergegevens in het kader van strafrechtelijke procedures. Het Verdrag besteedt ook aandacht aan de uitlevering voor feiten die in het Verdrag geregeld worden, waarbij de eis van dubbele strafbaarheid van toepassing is en een minimale strafbedreiging van een jaar gevangenisstraf. De Uitleveringswet moet met deze strafbare feiten worden uitgebreid. De bepalingen over internationale rechtshulp in het Wetboek van Strafvordering behoeven geen wijziging of aanvulling.

2.4. Welke wetswijzigingen zijn op materieelrechtelijk gebied nodig?

Wat betreft het materieelrechtelijke deel zijn wetswijzigingen nodig ten behoeve van een aantal artikelen van het Verdrag.

Artikel 2 (wederrechtelijke toegang) noopt tot aanpassing van artikel 138a Sr (computervredebreuk).

Artikel 3 (wederrechtelijke onderschepping) noopt tot aanpassing van de artikelen 139a t/m 139c Sr (aftappen en opnemen gegevens).

Artikel 4 (verstoring computergegevens) behoeft gelet op artikel 350a Sr (beschadiging etc. van computergegevens) niet tot aanpassing te leiden, met dien verstande dat de in het oorspronkelijke wetsvoorstel geschrapte zinsnede «dan wel andere gegevens daaraan toevoegt» bij nadere overweging beter gehandhaafd kan blijven om buiten twijfel te stellen dat het opzettelijk en wederrechtelijk invoeren van gegevens in een geautomatiseerd werk strafbaar blijft.

Artikel 5 (verstoring van computersystemen) wordt bestreken door de artikelen 350a Sr (beschadiging etc. van computergegevens) en 161sexies en 161septies Sr (vernieling van geautomatiseerde werken ten algemenen nutte) en door het in onderhavige Wetsvoorstel Computercriminaliteit II voorgestelde nieuwe artikel 138b, maar om artikel 5 van het Verdrag ten volle te implementeren is een aanpassing van dat nieuwe artikel 138b wenselijk.

Artikel 6 (voorbereidingshandelingen voor de feiten bedoeld in de artikelen 2 t/m 5) wordt voor een deel bestreken door de artikelen 139d (plaatsen aftapapparatuur), 350a en 350b (beschadiging etc. computergegevens) en voor een deel door de algemene voorbereidingsbepaling van artikel 46 Sr (voor zover het gaat om de voorbereiding van misdrijven waarop 8 jaar of meer staat), maar noopt niettemin tot een bijzondere aanvulling van de artikelen 139d en 161sexies.

De artikelen 7 (vervalsing van computergegevens) *en 8* (computergerelateerde fraude) hebben ten doel in de elektronische omgeving strafbaar te maken wat in de stoffelijke wereld al strafbaar is. De artikelen 225 en 226 (valsheid in geschrift; geschrift wordt door de jurisprudentie breed geïnterpreteerd) en artikel 232 (valse betaalkaart/waardekaart), zoals dat recent is gewijzigd door de Wet van 21 april 2004 (Stb. 180) en zoals dat door het onderhavige wetsvoorstel nog gewijzigd zal worden, voorzien in belangrijke mate hierin, in samenhang met de algemene bepalingen over oplichting e.d. (artikelen 326 Sr ev).

Aan *artikel 9* (misdrijven in verband met kinderpornografie) wordt in de Nederlandse wetgeving voldaan door de nog recent aangescherpte bepaling in artikel 240b Sr.

Aan *artikel 10* (auteursrechtelijke misdrijven) wordt voldaan door de huidige strafbepalingen in de Auteurswet 1912 en de Wet op de naburige rechten.

Tenslotte verdient in dit verband *artikel 22* (rechtsmacht) nog de aandacht. Het Wetboek van Strafrecht voorziet grotendeels in de rechtsmacht zoals omschreven in het eerste lid van dat artikel, namelijk voor zover het betreft de onderdelen a tot en met c en het *eerste* deel van onderdeel d. Het *laatste* deel van onderdeel d betreft de rechtsmacht over computerdelicten, door (Nederlandse) onderdanen begaan buiten de territoriale rechtsmacht van enige Staat. Ons wetboek kent op dit moment een dergelijke rechtsmacht niet. Daarom is het wenselijk artikel 5 Sr op dit punt aan te vullen.

2.5 Welke wijzigingen zijn op strafvorderlijk gebied nog nodig?

Wat betreft het strafvorderlijke deel zijn op enkele onderdelen wetswijzigingen nodig ten behoeve van het Verdrag.

Aanvulling van het Wetboek van Strafvordering is nodig om ten volle tegemoet te komen aan *artikel 14* van het Verdrag (reikwijdte van de procesrechtelijke maatregelen), met name het tweede lid, onderdeel a.

Artikel 15 (inzake voorwaarden en waarborgen) bepaalt dat de invoering, uitwerking en toepassing van de procedures en bevoegdheden onderworpen zijn aan de voorwaarden en waarborgen, vervat in het nationale recht, dat een passende bescherming moet bieden aan de rechten van de mens, met inachtneming van het proportionaliteitsbeginsel. Bij de introductie van nieuwe procedures en bevoegdheden moet dus worden voorzien in een adequaat stelsel van toepassingsvoorwaarden en waarborgen. Bij de bijgaande voorstellen wordt hieraan toepassing gegeven door, met inachtneming van het binnen ons strafvorderlijk systeem gebruikelijke systeem, uitdrukkelijk te bepalen in welke gevallen de bevoegdheid mag worden toegepast, welke autoriteit of autoriteiten daartoe bevoegd is of zijn en op welke wijze daartegen zonodig rechtsmiddelen kunnen worden aangewend.

Aanvulling van het Wetboek van Strafvordering is nodig om tegemoet te komen aan de *artikelen 16* (de tijdelijke bevriezing van bepaalde opgeslagen maar vluchtige gegevens, zonder dat de autoriteiten kennis kunnen nemen van de inhoud daarvan) *en 17* (de tijdelijke bevriezing en eventuele snelle ontsluiting van verkeersgegevens).

Geen wijziging of aanvulling van het Wetboek van Strafvordering is nodig voor *artikel 18* van het Verdrag (bevel om specifieke computergegevens waaronder abonneegegevens te verstrekken). Volstaan kan worden met de bestaande artikelen 126n en 126na (dit laatste artikel, ingevoegd bij de wet van 18 maart 2004 (Stb. 105) (vorderen gegevens telecommunicatie) heeft betrekking heeft op het vorderen van de zogenaamde «NAW-gegevens» (naam, adres etc.) en met de bepalingen die in het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441) worden voorgesteld om aan het Wetboek van Strafvordering toe te voegen; het betreft de voorgestelde artikelen 126nc tot en met 126nf van dat Wetboek.

Ook voor *artikel 19* van het Verdrag (de bevoegdheid om computers en computergegevens te doorzoeken en eventueel in beslag te nemen c.q. te kopiëren) is geen wijziging of aanvulling van het Wetboek van Strafvordering nodig. Volstaan kan worden met de huidige bepalingen inzake inbeslagneming en artikel 125i van het Wetboek van Strafvordering, zoals dat wordt gewijzigd door het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441).

Artikel 20 (het in «real-time» vergaren of vastleggen van verkeersgegevens) verplicht de verdragsluitende partijen enerzijds (a) tot het zelf in «real time» kunnen vergaren of vastleggen van verkeersgegevens en anderzijds (b) tot het nemen van maatregelen waardoor de service providers verplicht kunnen worden om in «real time» verkeersgegevens te vergaren of vast te leggen of daarbij de autoriteiten behulpzaam te zijn. En dit alles geldt, gelet op de betekenis van het begrip service provider in artikel 1 van het Verdrag, niet alleen voor de openbare telecomsector maar ook voor private netwerken en voor degenen die ten behoeve van die diensten computergegevens bewerken, verwerken of opslaan, zoals bijvoorbeeld de zogenaamde web-hosts.

De service provider

Ons wettelijk stelsel voorziet door middel van artikel 126n van het Wetboek van Strafvordering in de bevoegdheid van de officier van justitie om van de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst te vorderen, dat deze bepaalde gegevens verstrekt over een gebruiker en over het telecommunicatieverkeer met betrekking tot die gebruiker, de verkeersgegevens. Onze wetgeving voorziet jegens andere entiteiten die onder het ruime verdragsbegrip «service provider» vallen, niet in een dergelijke specifieke vordering. Voor die andere entiteiten kan gebruik worden gemaakt van de nieuwe, in het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441) voorgestelde artikelen 126nd en 126ne Sv. Die artikelen betreffen de bevoegdheid van de officier van justitie om van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, te vorderen deze gegevens te verstrekken. Deze bevoegdheid kan zich mede uitstrekken tot gegevens die eerst na het tijdstip van de vordering worden verwerkt en ten aanzien waarvan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, kan bepalen dat de gegevens direct na de verwerking worden verstrekt. Ik geef er echter de voorkeur aan, de vordering van verkeersgegevens voor de niet-openbare sector te regelen in het kader van artikel 126n Sv, in aansluiting op de regeling voor de openbare

telecomsector. Welke gegevens daadwerkelijk onder het bereik van artikel 126n Sv vallen, wordt vastgesteld bij het Besluit vorderen gegevens telecommunicatie (Stb. 2004, 394), dat zonodig zal moeten worden aangevuld voor zover het verkeersgegevens betreft die bij de niet-openbare sector worden gegenereerd.

De opsporingsautoriteiten zelf

Het vergaren of vastleggen van verkeersgegevens is doorgaans praktisch slechts mogelijk met medewerking van degenen die de verkeersgegevens genereren, dat wil zeggen de aanbieders.

Voor de met opsporing van strafbare feiten belaste autoriteiten is het eigenlijk ook niet nodig – en bovendien met de ten dienste staande technische mogelijkheden ook niet goed mogelijk – om «verkeersgegevens» zelf op te nemen zonder de medewerking van de betrokken dienst. In een dergelijk geval zal wellicht eerder behoefte bestaan aan de toepassing van bevoegdheden zoals doorzoekings- en inbeslagnemingsbevoegdheden.

Niettemin schrijft het Verdrag voor dat de opsporingsautoriteiten ook zelf bevoegd moeten zijn om verkeersgegevens die betrekking hebben op specifieke berichten, te vergaren of vast te leggen. Mede omdat in een dergelijk geval veelal ook behoefte zal bestaan aan onderzoek van de inhoud van de berichten, wordt voor de implementatie van dit onderdeel van het Verdrag aansluiting gezocht bij artikel 126m Strafvordering, dat in algemene zin betrekking heeft op onderzoek van (tele)communicatie en aan de toepassing waarvan zware eisen zijn gesteld. Gelet op de samenhang met artikel 21 van het Verdrag, zij verwezen naar de toelichting op de implementatie van dat artikel hieronder.

Artikel 21 (het in «real-time» vergaren of vastleggen van gespecificeerde inhoudgegevens) gaat er, evenals artikel 20, vanuit dat de opsporingsautoriteiten beschikken over eigen bevoegdheden en dat daarnaast een medewerkingsplicht komt te rusten op de service providers. Hier gaat het evenwel niet om verkeersgegevens maar om de inhoud van specifieke berichten.

Wat betreft de bevoegdheden van de opsporingsautoriteiten zijn in ons rechtstelsel van belang de artikelen 126l en 126m Sv. Artikel 126l biedt de grondslag voor het met een technisch hulpmiddel, zoals bijvoorbeeld een op het toetsenbord aangebrachte «bug», opnemen van vertrouwelijke communicatie; het is hierbij irrelevant op welke wijze de communicatie plaatsvindt en in het algemeen is het nodig om buiten medeweten van de betrokkene een plaats te betreden. Artikel 126m biedt de grondslag voor het met een technisch hulpmiddel zoals een tapkamer opnemen van telecommunicatie via een openbaar telecommunicatienetwerk dan wel met gebruikmaking van openbare telecommunicatiediensten.

Kenmerkend voor het huidige artikel 126m is – in de woorden van de commentatoren in Cleiren/Nijboer 200. (Tekst en Commentaar Sv, artikel 126m, aantekening 1) – dat voor de effectuering van de bevoegdheid de medewerking van de aanbieder van telecommunicatie nodig is maar dat tegelijkertijd met het gebruik van de faciliteiten van de aanbieder kan worden volstaan voor de effectuering van de bevoegdheid. Teneinde te voldoen aan de eisen van het Verdrag – ook thans blijkt hieraan in de praktijk overigens reeds behoefte te bestaan, zoals het OM in zijn advies opmerkte – wordt dit kenmerkende karakter van artikel 126m in die zin gewijzigd, dat het opnemen van telecommunicatie voortaan zowel kan plaatsvinden met medewerking van de aanbieder – met inachtneming van de Telecommunicatiewet – als zonder die medewerking. Met het oog op het opnemen van communicatie in een besloten netwerk – waarover het Verdrag zich ook uitstrekt – wordt de werking van artikel 126m in die zin verbreed dat de bevoegdheid zich niet alleen uitstrekt tot telecommuni-

catie die plaatsvindt met gebruikmaking van openbare netwerken of diensten, maar in den brede tot communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst. In aansluiting op artikel 1 van het Verdrag wordt daaronder verstaan: degene die aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

De bevoegdheid blijft toegekend aan de officier van justitie, na machtiging door de rechter-commissaris, en kan slechts worden toegepast 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. Gelet op de ingrijpendheid van de bevoegdheid en de uiteenlopende methoden met behulp waarvan deze kan worden toegepast, acht ik het wenselijk dat bovendien eisen worden gesteld aan de technische hulpmiddelen die kunnen worden ingezet voor het opnemen van de communicatie. Door een wijziging van artikel 126ee Sv wordt vastgelegd dat de hier bedoelde eisen worden gesteld bij algemene maatregel van bestuur.

2.6. De in het Verdrag opgenomen definities

Het Verdrag kent in artikel 1 een viertal definities. Het Verdrag verplicht er niet toe om de definities (al dan niet letterlijk) over te nemen in de nationale wetgeving.

In het Wetboek van Strafrecht zijn de termen computergegevens (artikel 80quinquies Sr) en geautomatiseerd werk (artikel 80sexies Sr) zodanig gedefinieerd dat daarmee volstaan kan worden. Deze definitiebepalingen zijn destijds bij amendement voorgesteld waarbij men zich er waarschijnlijk geen rekenschap van heeft gegeven dat deze ook gelding dienen te hebben voor het WvSv. De praktijk heeft inmiddels echter uitgewezen dat er geen behoefte bestaat aan een aparte definitiebepaling in het WvSv.

Het Verdrag definieert het begrip «service provider» om duidelijk te maken jegens welke entititeiten bepaalde strafvorderlijke bevoegdheden gehanteerd moeten kunnen worden. Het begrip wordt gedefinieerd als iedere publieke of private instelling die aan de gebruikers van haar diensten de mogelijkheid biedt te communiceren met behulp van een computersysteem en iedere andere instelling die computergegevens verwerkt of opslaat ten behoeve van (de gebruikers van) zo'n communicatiedienst. Bij dit laatste kan men bijv. denken aan de aanbieders van webhostingdiensten en beheerders van websites. Het WvSv voorziet in bevoegdheden ten opzichte van aanbieders van openbare telecommunicatienetwerken en -diensten in de zin van de Telecommunicatiewet. Daaronder worden verstaan de klassieke aanbieders van openbare telecommunicatienetwerken en -diensten en de aanbieders van internettoegang. Het Verdrag maakt geen onderscheid tussen openbare elektronische communicatiediensten en niet-openbare elektronische communicatiediensten en richt zich ook op aanbieders die gebruik maken van deze netwerken om hun diensten aan te bieden, zoals de beheerders en eigenaren van websites en webhostingdiensten. In een nieuw artikel in het WvSv wordt daartoe een definitie opgenomen van het begrip «aanbieder van een communicatiedienst», waarbij nauw wordt aangesloten bij de begripsbepaling in het Verdrag.

In het Verdrag is vervolgens het begrip «verkeersgegevens» gedefinieerd, een begrip dat ook van belang is voor de regeling van strafvorder-

lijke bevoegdheden, met name de artikelen 126n en 126u van het Wetboek van Strafvordering. Bij die artikelen is bepaald dat bij algemene maatregel van bestuur de gegevens worden aangewezen waarop de in die artikelen bedoelde vorderingen betrekking kunnen hebben. Dit is gedaan bij het Besluit vorderen gegevens telecommunicatie (Stb. 2004, 394). De in dat besluit vermelde gegevens sluiten aan bij het begrip verkeersgegevens in de betekenis van het Cybercrime Verdrag. Deze gegevens omvatten mede de zogenaamde gebruikersgegevens. In zoverre wijkt de terminologie van het Cybercrime Verdrag en van het bedoelde besluit af van de definitie van verkeersgegevens in artikel 11.1 van de Telecommunicatiewet, waarbij de gebruikersgegevens geen onderdeel vormen van de verkeersgegevens.

Het Verdrag kent in artikel 18 overigens nog een vijfde definitie, nl. die van abonneegegevens. Gelet op de hiervoor genoemde algemene maatregel van bestuur en op artikel 126na van het Wetboek van Strafvordering (ingevoegd bij de Wet vorderen gegevens telecommunicatie) is een nadere definitie van deze gegevens niet nodig.

3. Toelichting op de nota van wijziging

3.1. Inpassing in het Nederlandse stelsel

3.1.1 Strafrecht

Zoals hiervoor in de paragrafen 2.3 tot en met 2.5 al aan de orde kwam, is bezien in hoeverre ons Wetboek van Strafrecht voorziet in strafbaarstelling van de feiten zoals omschreven in de artikelen 2 tot en met 12 van het Verdrag. Voor zover dat niet het geval is, wordt het Wetboek aangevuld. Artikel 13 van het Verdrag schrijft de verdragsluitende partijen vervolgens voor om te zorgen voor doeltreffende, proportionele en afschrikwekkende sancties, waaronder vrijheidsstraffen. Hoewel ons Wetboek in beginsel aan die eis voldoet – op alle relevante feiten is gevangenisstraf gesteld – is bezien of nog sprake is van voldoende afschrikwekkende werking van de sancties, mede gelet op het mogelijk grensoverschrijdende karakter van een aantal van de hier bedoelde strafbare feiten. Dit heeft ertoe geleid dat wordt voorgesteld de bestaande maximumstraf op computervredebreuk (artikel 138a, eerste lid, Sr) te verhogen van zes maanden tot 1 jaar. Ook in het nieuw voorgestelde artikel 138b Sr werd reeds gekozen voor een gevangenisstraf van ten hoogste een jaar. Ten aanzien van artikel 139d, eerste lid, Sr (het plaatsen van opname-, aftap- of afluisterapparatuur) wordt ook een verhoging voorgesteld van zes maanden naar een jaar. Voor het aan artikel 139d toe te voegen tweede lid (voorbereidingshandelingen, gericht op misdrijf als bedoeld in 138a, eerste lid, 138b of 139c Sr) wordt gekozen voor eenzelfde maximumstraf. En voor het aan artikel 139d toe te voegen derde lid (voorbereidingshandeling gericht op misdrijf als bedoeld in artikel 138a, tweede of derde lid) wordt aangesloten bij het maximum dat ook geldt voor overtreding van artikel 138a, tweede of derde lid, Sr, te weten vier jaar. In artikel 161sexies wordt zowel in het (bestaande) eerste lid als in het (nieuwe) tweede lid ook een maximum van een jaar gevangenisstraf voorgesteld.

3.1.2 Strafvordering; nieuwe bevoegdheden en de daarvoor geldende voorwaarden en waarborgen

3.1.2.a Inleiding

Zoals in de paragrafen 2.3 tot en met 2.5 werd vermeld, is wat betreft de strafvorderlijke bevoegdheden bezien in hoeverre ons Wetboek van

Strafvordering al voorziet in de bevoegdheden waartoe het Verdrag verplicht. Waar zulks nodig is ter uitvoering van artikel 14 van het Verdrag, worden in deze nota van wijziging aanvullende bevoegdheden voorgesteld. Artikel 15 van het Verdrag bepaalt vervolgens dat de verdragsluitende partijen erop toezien dat de invoering van de bedoelde bevoegdheden worden onderworpen aan de voorwaarden en waarborgen, vervat in hun nationale recht, dat onder meer een passende bescherming moet bieden aan de rechten van de mens. In het onderstaande zal daarop worden ingegaan.

3.1.2.b De nieuwe bevoegdheden

Om welke bevoegdheden gaat het in feite?

– In de artikelen 126m en 126t wordt, naast de reeds bestaande bevoegdheid om mèt medewerking van de aanbieder telecommunicatie op te nemen, de mogelijkheid geïntroduceerd om zonder medewerking van de aanbieder telecommunicatie op te nemen; daarnaast wordt de werking van deze artikelen uitgebreid tot communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst in de zin van het nieuwe artikel 126la Sv, bijvoorbeeld geheel of gedeeltelijk besloten netwerken.

– In de artikelen 126n en 126u wordt de bevoegdheid om verkeersgegevens te vorderen uitgebreid tot de aanbieders van een communicatiedienst in de zin van artikel 126la Sv.

– In nieuwe artikelen 126ni en 126ui wordt de bevoegdheid geïntroduceerd, te vorderen dat bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk, voor een periode van ten hoogste negentig dagen worden bewaard en beschikbaar gehouden (het zgn. «bevriezingsbevel»).

3.1.2.c Toetsing aan artikel 8 EVRM

Bevoegdheden die een inbreuk kunnen maken op het recht op bescherming van de persoonlijke levenssfeer, dienen getoetst te worden aan artikel 8, tweede lid, van het EVRM, dat bepaalt dat een beperking van het recht op eerbiediging van de persoonlijke levenssfeer alleen is toegestaan voor zover daarin bij de wet is voorzien en dit in een democratische samenleving noodzakelijk is in het belang van enkele met name genoemde doelen, waaronder het voorkomen van strafbare feiten. Zoals bekend wordt onder dat laatste criterium de strafvorderlijke afwikkeling van strafbare feiten – waaronder de opsporing ervan- mede begrepen. Bij de eis dat inmenging in de persoonlijke levenssfeer noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid, die een afweging moet maken of regeling van de bevoegdheid nodig is voor de opsporing van strafbare feiten. Hierbij dient te worden afgewogen of het individuele belang van de burger bij bescherming van de persoonlijke levenssfeer in bepaalde gevallen minder zwaar dient te wegen dan het algemene belang van de opsporing van strafbare feiten. In algemene zin is deze afweging voor de hier bedoelde bevoegdheden uitdrukkelijk gemaakt bij de voorbereiding en totstandkoming van het Cybercrime Verdrag. De voorgestelde bevoegdheden zijn bij de huidige stand van zaken, gelet op de technologische ontwikkelingen, inderdaad noodzakelijk voor de opsporing van tal van strafbare feiten, niet alleen van computercriminaliteit in enge zin maar ook van strafbare feiten die door middel van computersystemen worden begaan en in algemene zin van strafbare feiten waarvoor relevant bewijsmateriaal in elektronische vorm is opgeslagen.

In het onderstaande wordt nader ingegaan op de nieuwe bevoegdheden en op de waarborgen en beperkingen die daarbij gelden; ik verwijs ook

naar de toelichting op onderdeel 15 van de nota van toelichting in paragraaf 3.2 hierna.

– *De artikelen 126m en 126t*

De uitbreiding van de werking van de artikelen 126m en 126t vloeit voort uit artikel 21, eerste lid, sub a, van het Verdrag, in samenhang met de begripsbepaling van «service provider» in artikel 1 van het Verdrag.

Op grond van artikel 126m Sv bestaat thans reeds de bevoegdheid om te bevelen dat telecommunicatie, die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van openbare telecommunicatiediensten, wordt opgenomen met een technisch hulpmiddel. Daarbij is, conform de Telecommunicatiewet, voorzien in medewerking die moet worden verleend door de aanbieder. Het Verdrag noopt ertoe deze mogelijkheid ook te introduceren voor communicatie die plaatsvindt via niet-openbare netwerken en diensten en tevens mogelijk te maken dat opsporingsautoriteiten zelf, zonder medewerking van de aanbieder, de inhoud van dergelijke communicatie opnemen. Dat zijn vergaande bevoegdheden, omdat het besloten netwerken betreft en omdat communicatie kan worden opgenomen zelfs zonder dat de aanbieder daarvan afweet. In dit opzicht is een vergelijking mogelijk met artikel 126l Sv.

Daarom worden de bevoegdheden, op te nemen in de nieuw geformuleerde artikelen 126m en 126t, sterk genormeerd en wordt voorzien in adequate waarborgen en aanvullende eisen.

– De bevoegdheid mag slechts worden gehanteerd 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, waarbij ook nog de toets moet plaatsvinden dat het onderzoek het gebruik van de bevoegdheid dringend vordert.

– De bevoegdheid ligt bij de officier van justitie.

– Maar deze kan het bevel slechts geven na schriftelijke machtiging van de rechter-commissaris, die daarbij toetst of wordt voldaan aan de eisen die zijn gesteld.

– Het bevel kan tenslotte slechts voor een beperkte tijdsduur worden gegeven, waarna uitdrukkelijk verlenging nodig is met opnieuw inschakeling van de rechter-commissaris.

– Aan al deze in artikel 126m vermelde eisen wordt door middel van een wijziging van artikel 126ee bovendien de specifieke eis toegevoegd dat, indien communicatie buiten medeweten van de aanbieder wordt opgenomen, het daartoe te gebruiken technische hulpmiddel moet voldoen aan bij algemene maatregel van bestuur te stellen regels, waarbij moet worden gedacht aan technische eisen, protocollering, controle op de naleving en dergelijke.

– De notificatieplicht, geregeld in artikel 126bb Sv, is van toepassing.

– Ook de beklagmogelijkheid van artikel 552a Sv is van toepassing.

Alles bijeen genomen meen ik dat de bevoegdheid de toets aan artikel 8 EVRM kan doorstaan.

– *Artikelen 126n en 126u*

De uitbreiding van de werking van de artikelen 126n en 126u vloeit voort uit artikel 20, eerste lid, sub a, van het Verdrag, in samenhang met de begripsbepaling van «service provider».

Deze uitbreiding betekent dat verkeersgegevens kunnen worden gevorderd niet alleen van de aanbieders van openbare telecommunicatienetwerken of -diensten, maar ook van andere aanbieders van een communicatiedienst in de zin van het nieuw voorgestelde artikel 126la. Anders dan bij de artikelen 126m en 126t gaat het hierbij niet om inhoudelijke gegevens maar slechts om verkeersgegevens. Daar komt bij dat, anders dan bij de openbare telecommunicatiesector, bij de geheel of

gedeeltelijk besloten netwerken en diensten door de aanbieder niet altijd verkeersgegevens zullen worden gegenereerd. De betekenis van deze bepaling voor de praktijk zal naar verwachting dan ook gering zijn. Niettemin is, naar aanleiding van adviezen, ten opzichte van het ter consultatie voorgelegde voorstel een begrenzing aangebracht in de kring van degenen van wie de verkeersgegevens kunnen worden gevorderd, te weten degenen die kunnen worden aangemerkt als aanbieders van de communicatiedienst. Als er geen verkeersgegevens zijn of als de aanbieders daartoe geen toegang hebben, kan de vordering niet gegeven en in ieder geval niet opgevolgd worden. Voor het geval een vordering wel gegeven kan worden, biedt artikel 126n de nodige waarborgen:

– Er moet sprake zijn van een verdenking van een misdrijf als bedoeld in artikel 67 Sv;

– De vordering mag slechts worden gegeven in het belang van het onderzoek;

– De vordering kan slechts betrekking hebben op gegevens die uitdrukkelijk bij algemene maatregel van bestuur zijn aangegeven;

– verschoningsgerechtigde personen hoeven niet aan het bevel te voldoen;

– De vordering is in de tijd beperkt;

– In het proces-verbaal moet de toepassing volgens nauw omschreven standaarden verantwoord worden;

– De officier van justitie moet bij de vordering voldoen aan de nader bij algemene maatregel van bestuur te stellen eisen.

– Tenslotte is de notificatieplicht van artikel 126aa van toepassing, evenals de beklagmogelijkheid van artikel 552a Sv.

Alles bijeen genomen meen ik dat hiermee is voorzien in zodanige voorwaarden en waarborgen dat de bevoegdheden de toets aan artikel 8 EVRM kunnen doorstaan.

– *Artikelen 126ni en 126ui*

De introductie van de zgn. bevriezingsbevelen in de artikelen 126ni en 126ui vloeit voort uit de artikelen 16 en 17 van het Verdrag. Voorstellen voor bevriezingsbepalingen werden reeds gedaan in het rapport «Gegevensvergaring in strafvordering» van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij. In het kabinetsstandpunt over dat rapport (Kamerstukken II 2001/02, 28 366, nr. 1, blz. 20 t/m 22) is uitvoerig op die voorstellen en op de daarover gegeven adviezen ingegaan. De in de nota van wijziging opgenomen teksten sluiten nauw aan bij de bedoelde voorstellen, met inbegrip van de wijzigingen die werden vermeld in het bedoelde kabinetsstandpunt. Zo is een maximumtermijn van 90 dagen opgenomen en is de bevoegdheid niet neergelegd bij de hulpofficier maar bij de officier van justitie. Verwezen zij naar het bedoelde kabinetsstandpunt.

3.2. Toelichting op de onderdelen van de nota van wijziging

De nota van wijziging is ingedeeld in Arabische nummers.

– Nummer 1 betreft het opschrift en de considerans van het wetsvoorstel.

– De nummers 2 tot en met 14 betreffen wijzigingen in artikel I van het wetsvoorstel (inzake het Wetboek van Strafrecht).

– De nummers 15 tot en met 24 betreffen wijzigingen in artikel II van het wetsvoorstel (inzake het Wetboek van Strafvordering).

– Nummer 25 betreft de invoeging van een nieuw artikel IIA in het wetsvoorstel (inzake de Uitleveringswet).

– Nummer 26 betreft een wijziging van artikel III van het wetsvoorstel (inzake de Telecommunicatiewet).

– Nummer 27 betreft artikel IV (het overgangsrecht) van het wetsvoorstel.

– Nummer 28 betreft een wijziging in een inmiddels in werking getreden wijzigingswet respectievelijk in een voorstel van een wijzigingswet.

1. (Wijziging opschrift en considerans)

Het opschrift en de considerans van het wetsvoorstel worden gewijzigd omdat ook de Uitleveringswet moet worden gewijzigd.

1a. (Nieuw onderdeel A, strekkende tot wijziging van artikel 5 Sr)

Artikel 22 van het Verdrag verplicht de Partijen ertoe, rechtsmacht te vestigen met betrekking tot de strafbare feiten die in het Verdrag zijn benoemd, en wel voor de volgende gevallen:

a. wanneer het feit wordt begaan op haar grondgebied;

b. wanneer het feit wordt begaan aan boord van een schip dat de vlag van die Partij voert;

c. wanneer het feit wordt begaan aan boord van een luchtvaartuig dat onder de wetten van die Partij is geregistreerd; of

d. wanneer het strafbare feit wordt begaan door een van haar onderdanen, indien het feit strafbaar is onder de strafwet van de Staat waar het is begaan of indien het feit is begaan buiten de territoriale rechtsmacht van enige Staat.

Ons Wetboek van Strafrecht voorziet grotendeels in deze rechtsmacht. Onderdeel a is geregeld in artikel 2 Sr. De onderdelen b en c zijn geregeld in artikel 3 Sr. Onderdeel d is wat betreft de eerste zinsnede (het feit is strafbaar onder de strafwet van de Staat waar het is begaan) geregeld in artikel 5, eerste lid, onderdeel 2*, Sr. Alleen het tweede deel van onderdeel d is in ons Wetboek van Strafrecht niet geregeld. Het betreft computerdelicten, door Nederlandse onderdanen begaan buiten de territoriale rechtsmacht van enige Staat. Praktisch gesproken gaat het hierbij om gevallen waarin Nederlanders buiten de territoriale rechtsmacht van enig land computerdelicten begaan aan boord van een niet onder enige vlag geregistreerd vaar- of luchtvaartuig.

Weliswaar opent artikel 22 van het Verdrag de mogelijkheid terzake een voorbehoud op te nemen, maar gelet op de doelstelling van het Verdrag is het wenselijk zoveel mogelijk aan te sluiten bij het in het Verdrag gekozen stelsel van toedeling van nationale rechtsmacht. Daarbij is van belang dat de aansluiting kan worden bereikt met een geringe aanpassing van artikel 5 Sr, die strikt wordt beperkt tot de feiten zoals benoemd in het Cybercrime Verdrag. De onderhavige aanvulling van artikel 5 strekt daartoe.

2. (Wijziging onderdeel D van wetsvoorstel inzake artikel 138a Sr; betreft artikel 2 Verdrag)

Artikel 2 van het Verdrag verplicht de staten ertoe de opzettelijke en wederrechtelijke toegang tot een computersysteem of onderdeel daarvan strafbaar te stellen. Artikel 2 biedt de verdragsluitende partijen weliswaar de mogelijkheid om aanvullende eisen aan de strafbaarheid te stellen in die zin dat een staat mag eisen dat het feit wordt gepleegd (1) door een beveiliging te doorbreken, (2) met het oogmerk om computergegevens te verkrijgen of (3) met een andere «dishonest intent», maar in dit verband moeten wij ook rekening houden met de eisen die worden gesteld door artikel 2 van het Kaderbesluit 2003/../JGZ van de Raad van de EU inzake aanvallen op informatiesystemen (PB ..). Ook dat artikel schrijft namelijk voor, maatregelen te treffen om opzettelijke onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan strafbaar te stellen, maar het Kaderbesluit laat geen grote vrijheid aan de lidstaten bij de inrichting van de strafbepaling. Het Kaderbesluit laat de keuze tussen een algehele strafbaarstelling zonder enige beperking en een strafbaarstelling

waarbij alleen de beperking wordt aangebracht dat het feit dient plaats te vinden door een doorbreking van een beveiliging. Deze laatste modaliteit acht ik, mede gelet op het thans geldende artikel 138a Sr, waarin naast de doorbreking van een beveiliging ook andere elementen worden genoemd die kunnen leiden tot «computervredebreuk», te beperkt en daarom onwenselijk. Artikel 138a Sr stelt immers als aanvullende eis voor strafbaarheid, dat hetzij een beveiliging is doorbroken, hetzij de toegang is verworven door een technische ingreep, met hulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.

Mede met het oog op een zo krachtig mogelijke bestrijding van het verschijnsel «hacking» acht ik het daarom wenselijk geen beperking aan te brengen maar artikel 138a zodanig te herformuleren, dat in beginsel ieder opzettelijk en wederrechtelijk binnendringen in een computer(systeem) bestraft kan worden. Daarom stel ik voor de onderdelen a en b van artikel 138a, die thans nog als voorwaarde voor strafbaarheid zijn geformuleerd, te formuleren als *voorbeelden* van gevallen waarin sprake is van «binnendringen», door aan te geven dat in die gevallen in ieder geval sprake is van binnendringen in de zin van dit artikel. Daarmee wordt voor de jurisprudentie de nodige ruimte geschapen om ook andere methoden waarmee toegang wordt verworven, als binnendringen aan te merken. Het doet mij genoegen dat de NVVR het voordeel onderkent dat op deze wijze de nodige ruimte wordt gelaten voor nieuwe technologische ontwikkelingen.

Voor de goede orde merk ik naar aanleiding van het advies van het OM nog op dat de onderhavige bepaling in strikte zin geen definitiebepaling betreft die noodzakelijkerwijs in de betekenistitel van het Wetboek van Strafrecht opgenomen zou moeten worden. Bovendien kent het Wetboek van Strafrecht ook thans reeds strafbepalingen waarin uitleg wordt gegeven aan de in die strafbepaling gehanteerde terminologie, zoals de artikel 361, 420bis, 437 etc.

Naar aanleiding van het advies van de NOvA ga ik in het onderstaande nader in op het begrip «technische ingreep», dat ook thans in artikel 138a voorkomt maar dat bij de introductie daarvan door de wetgever niet van een toelichting is voorzien.

Het bestanddeel «technische ingreep» is indertijd ontleend aan artikel 326c Sr, dat bij nota van wijziging (Kamerstukken II 1990/91, 21 551, nr. 7, onderdeel Ia) werd geïntroduceerd in het toenmalige wetsvoorstel inzake computercriminaliteit, echter zonder nadere toelichting. Het bestanddeel vindt volgens de toelichting bij de nota van wijziging (idem, blz. 5) zijn oorsprong in artikel 50, derde lid, van de toenmalige Wet op de telecommunicatievoorziening, dat de basis vormde van het commune delict (artikel 326c Sr) en dat met de wet inzake computercriminaliteit werd ingetrokken. Het bestanddeel is in artikel 138a Sr terechtgekomen met het overbrengen van bepaalde in de tekst van artikel 326c impliciet besloten hackingshandelingen naar artikel 138a Sr met de tweede nota van wijziging (21 551, nr. 12, onderdeel A). Voor een toelichting op het onderdeel moet derhalve worden teruggegaan naar de toelichting op artikel 50, derde lid, van de toenmalige Wet op de telecommunicatie-voorziening (20 369, nr. 3, blz. 53). Dat artikel betrof de strafbaarstelling van een specifiek op telecommunicatie toegespitste vorm van oplichting. Met het begrip «technische ingreep» werd gedoeld op elke vorm van technische manipulatie, zowel van buitenaf als in de telecommunicatie-infrastructuur en de draadomroepinrichting, die leidde tot het verrichten van de daar bedoelde diensten, ook waar dit gevolg werd bereikt louter ten gevolge van het door een technische ingreep rechtstreeks in werking stellen van een mechanisme (20 369, nr. 3, blz. 53). De «technische ingreep» was derhalve een vertaling van de oplichtingsmiddelen naar de technische omgeving van telecommunicatie.

Toegespitst op artikel 138a betekent dit het volgende. Het verwerven van toegang tot een geautomatiseerd werk door een technische ingreep veronderstelt een ingreep in c.q. het manipuleren van het technisch functioneren van het geautomatiseerde werk. Het louter intoetsen van een (al of niet vals) wachtwoord zal aldus niet als een technische ingreep kunnen worden beschouwd, omdat de afhandeling daarvan de functionaliteit van het systeem intact laat. Maar het intoetsen van een combinatie van tekens die als doel heeft het technisch functioneren van het geautomatiseerde werk zodanig te veranderen dat, ondanks het ontbreken van het juiste wachtwoord, toegang verworven kan worden, kan onder omstandigheden wel als technische ingreep worden beschouwd. In een dergelijk geval zal ook sprake kunnen zijn van het doorbreken van een beveiliging en/of van het gebruik van valse signalen of een «valse sleutel». Een nauw omlijnde interpretatie van deze begrippen is echter, zeker in de nieuwe opzet van artikel 138a, van beperkte betekenis, aangezien de rechter de vrijheid wordt gelaten om ook in andere gevallen vast te stellen dat sprake is van «binnendringen» in de zin van die bepaling.

In het oorspronkelijke wetsvoorstel werd artikel 138a, eerste lid, reeds in tweeërlei opzicht gewijzigd. Tussen de woorden «opzettelijk» en «wederrechtelijk» werd het woord «en» geplaatst en de woorden «voor de opslag of verwerking van gegevens» werden geschrapt. Beide wijzigingen zijn in het nieuwe tekstvoorstel verwerkt. De NVvR vroeg zich af of de oorspronkelijke tekst («opzettelijk wederrechtelijk») niet beter zou aansluiten bij artikel 2 van het Verdrag. Het springende punt hierbij is de vraag of de opzet als zodanig ook gericht moet zijn op de wederrechtelijkheid, wat een zware eis zou zijn. Weliswaar laat de Engelse verdragstekst deze interpretatie wellicht open, maar het *Explanatory Memorandum* (in het bijzonder onder nummer 47) geeft geen aanwijzingen voor een dergelijke strikte interpretatie. Daar komt bij dat in de Franse tekst van artikel 2 de opzet en de wederrechtelijkheid uitdrukkelijk nevengeschikt zijn («intentionnel et sans droit»). In de Nederlandse vertaling van het Verdrag wordt hierbij aangesloten. Ik meen dan ook dat de tussenvoeging van het woord «en» gehandhaafd moet blijven.

Tenslotte wordt, zoals reeds vermeld in de paragrafen 2.2 en 3.1, de strafmaat van artikel 138a, eerste lid, verhoogd van ten hoogste zes maanden naar ten hoogste een jaar gevangenisstraf.

3. (Wijziging onderdeel E wetsvoorstel inzake concept-artikel 138b Sr; betreft artikel 5 Verdrag)

Artikel 5 van het Verdrag heeft betrekking op de strafbaarstelling van de schending van de integriteit van computersystemen. Artikel 3 van het EU-kaderbesluit heeft hierop eveneens betrekking. Artikel 5 van het Verdrag spreekt over «the serious hindering of the functioning of a computer system», artikel 3 van het Kaderbesluit over «het ernstig hinderen of het onderbreken van de werking van een informatiesysteem». Het moet hierbij dus gaan om ernstige vormen van hinder voor de gebruiker. Gedacht kan worden aan het toezenden van gegevens aan een computer(systeem) in een zodanige vorm of omvang of met een zodanige frequentie dat dit een significant nadelig effect heeft op de mogelijkheid van de eigenaar of gebruiker om de computer (of het computersysteem) te gebruiken of te communiceren met andere systemen. Zo bestaan er programma's die zogenaamde »*denial of service*» aanvallen opwekken; programma's (bijvoorbeeld virussen) die het gebruik van computersystemen onmogelijk maken of dit substantieel vertragen; programma's die grote hoeveelheden e-mail sturen met als doel de communicatiefuncties van een systeem te verstoren.

In het Wetsvoorstel «Computercriminaliteit II» werd een nieuw artikel

138b voorgesteld, dat zich richtte op het opzettelijk en wederrechtelijk aan een ander toezenden van gegevens die bestemd zijn om de toegang van die ander tot een openbaar telecommunicatienetwerk of tot een openbare telecommunicatiedienst te belemmeren. Een dergelijk artikel is in het licht van artikel 5 van het Verdrag te beperkt. Daarom wordt nu een herzien artikel 138b voorgesteld dat, tezamen met artikel 350a Sr, de onderhavige materie bestrijkt. De term «belemmeren» geeft een adequate invulling aan de in het Verdrag en het kaderbesluit gehanteerde termen.

Het artikel ziet daarmee – ik merk dit op naar aanleiding van het advies van de NVVR – tevens op het «bombarderen» van *servers* en computers met e-mail, mits de opzet erop gericht is de toegang daartoe of het gebruik daarvan te belemmeren.

Voor de goede orde merk ik op dat in situaties waarop het verdragsartikel betrekking heeft ook het bestaande artikel 161sexies Strafrecht van toepassing kan zijn. Dat artikel betreft, voor zover hier van belang, de strafbaarstelling van degene die opzettelijk een computer(systeem) vernielt, beschadigt of onbruikbaar maakt of een stoornis in de gang of in de werking veroorzaakt, maar beperkt de strafbaarstelling tot gevallen waarin hetzij sprake is van een openbaar belang (gegevensverwerking ten algemenen nutte, onderdeel 1) hetzij gemeen gevaar voor goederen (onderdeel 2) of levensgevaar (onderdelen 3 en 4) te duchten is.

4, 5 en 6. (Wijziging onderdelen F, G en H wetsvoorstel, inzake de artikelen 139a, 139b en 139c Sr; betreft artikel 3 Verdrag)

Artikel 3 van het Verdrag betreft de onrechtmatige onderschepping, met technische middelen, van niet-publieke overbrenging van computergegevens naar, vanuit en binnen computersystemen. Het artikel beoogt daarmee een zo volledig mogelijke bescherming van de persoonlijke levenssfeer bij gegevensoverdracht. Het artikel – dat aansluit bij artikel 8 van het EVRM – betreft alle vormen van elektronische gegevensoverdracht, of deze nu plaatsvindt per telefoon, telefax, e-mail of andere overdracht van gegevensbestanden.

Het artikel heeft betrekking op «niet-publieke» gegevensoverdracht. De term «niet-publiek» heeft betrekking op de aard van het overdrachtsproces (communicatie) en niet op de aard van de gegevens. Denkbaar is een situatie waarin partijen vertrouwelijk wensen te communiceren over gegevens die op zichzelf openbaar beschikbaar zijn.

De term «niet-publiek» sluit op zichzelf niet communicatie via openbare netwerken uit. Communicatie tussen werknemers, al of niet voor zakelijke doeleinden, die te beschouwen is als «niet-publieke overdracht van computergegevens», wordt ook beschermd tegen wederrechtelijke onderschepping. De vraag of een onderschepping van communicatie tussen werknemers wederrechtelijk is, moet mede beantwoord worden in het licht van de concrete situatie, waaronder de arbeidsverhouding tussen werknemer en werkgever (zie ook ECRM Halford vs. UK, 25 juni 1997, 20605/92).

De communicatie in de vorm van de overdracht van computergegevens kan plaatsvinden binnen een enkel computersysteem, tussen twee computersystemen die al of niet aan verschillende personen toebehoren, tussen twee computers binnen een systeem, of tussen een computer en een persoon (door middel van het toetsenbord). De formulering van artikel 3 maakt duidelijk dat daaronder alle gegevensstromen vallen.

Onder technische middelen zijn alle hulpmiddelen begrepen die deze gegevenstromen zichtbaar kunnen maken en de inhoud ervan ter beschikking van de handelende persoon brengen, dus bij voorbeeld ook het waarnemen van de zogenaamde residustraling bij beeldschermen of de analyse van chips met behulp van infrarood-apparatuur.

In het Wetboek van Strafrecht is hier, als uitwerking van artikel 13 Grondwet, vooral het huidige artikel 139c (verbod om gegevens, die d.m.v. openbaar telecomnetwerk worden overgedragen maar die voor een ander bestemd zijn, op te nemen of af te tappen) van toepassing. Dat artikel is evenwel alleen van toepassing op gegevens die door middel van een openbaar telecommunicatienetwerk of door middel van daarop aangesloten randapparatuur worden overgedragen en dus niet op datacommunicatie in besloten netwerken, zoals bedrijfsnetwerken. De artikelen 139a, tweede lid (verbod om met een technisch hulpmiddel gegevens die in een woning d.m.v. een geautomatiseerd werk worden overgedragen, af te tappen of op te nemen), en 139b, tweede lid (verbod om met een technisch hulpmiddel gegevensoverdracht elders dan in een woning d.m.v. een geautomatiseerd werk heimelijk af te tappen of op te nemen) bieden weliswaar enig soelaas, zoals ook mijn ambtsvoorganger bij eerdere gelegenheid mededeelde (Kamerstukken II 2000/01, 23 530, nr. 45, blz. 6), maar artikel 139a is alleen van toepassing op woningen, besloten lokalen en erven, terwijl artikel 139b zich beperkt tot «heimelijk» aftappen en opnemen. Beide beperkingen laten zich niet verenigen met artikel 3 van het Verdrag. Hierin heb ik aanleiding gevonden om de artikelen 139a, 139b en 139c zodanig te herzien dat de materie die wordt geregeld in artikel 3 van het Verdrag in zijn geheel wordt bestreken door een nieuw geformuleerd artikel 139c.

Artikel 139a regelt voortaan derhalve nog louter het met een technisch hulpmiddel afluisteren en opnemen van gesprekken in woningen, besloten lokalen en erven, en artikel 139b het met een technisch hulpmiddel heimelijk afluisteren en opnemen van gesprekken elders. Beide artikelen zijn niet van toepassing op het aftappen en opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk. Dat wordt namelijk in zijn geheel geregeld in het nieuw geformuleerde artikel 139c. Strafbaar wordt gesteld hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk. Het dient hierbij dus te gaan om gegevens die «niet bestemd» zijn voor degene die aftapt of opneemt. Dat begrip omvat mede de gegevens die niet «mede» bestemd zijn voor degene die aftapt of opneemt. De uitsluiting van strafbaarheid van degene die in opdracht werkt van degene voor wie de gegevens (mede) bestemd zijn, wordt in de nieuwe bepaling geregeld door invoeging van het begrip wederrechtelijk. Degene die in opdracht van een gerechtigde handelt, handelt niet wederrechtelijk. Voor de goede orde merk ik op dat het begrip telecommunicatie gebruikt wordt in een brede betekenis, als iedere vorm van overdracht, uitzending of ontvangst van gegevens via kabels, radio-elektrische weg dan wel door middel van optische of andere (elektromagnetische) systemen, met inbegrip van niet-openbare netwerken en diensten.

Overdracht van gegevens door middel van telecommunicatie zal veelal tevens plaatsvinden door middel van een geautomatiseerd werk, maar omdat deze begrippen elkaar niet geheel overlappen worden zij – evenals thans nog het geval is in artikel 139b, tweede lid – naast elkaar gebruikt.

Voor de inzichtelijkheid van de materie is een bijlage bijgevoegd (bijlage I) waarin wordt aangegeven hoe de artikelen 139a t/m 139c thans luiden en hoe zij komen te luiden indien de voorstellen tot wet worden verheven.

7. (Wijziging onderdeel I wetsvoorstel, inzake aanvulling artikel 139d Sr; betreft artikel 6 Verdrag)

Artikel 6 van het Verdrag betreft een onderwerp dat in in het kopje wordt aangeduid als «misbruik van technische hulpmiddelen». De verdragspartijen moeten strafbaar stellen het opzettelijk en wederrech-

telijk vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van (i) een technisch hulpmiddel (daaronder begrepen een computerprogramma) dat hoofdzakelijk ontworpen is c.q. hoofdzakelijk geschikt gemaakt is tot het plegen van een van de strafbare feiten van de artikelen 2 t/m 5 van het Verdrag of van (ii) een computerwachtwoord, toegangscode of soortgelijk gegeven waardoor een computersysteem of deel daarvan kan worden binnengedrongen. Voor het element «hoofdzakelijk» verwijs ik naar de memorie van toelichting bij het voorstel voor de goedkeuringswet van het Verdrag (Kamerstukken II 2004/05, ..). Eis voor strafbaarheid is volgens artikel 6, dat een en ander plaatsvindt «met de bedoeling» dat het desbetreffende object of gegeven wordt gebruikt met het doel om een strafbaar feit te plegen als bedoeld in de artikelen 2 tot en met 5 van het Verdrag.

In feite gaat het hier om de strafbaarstelling van een aantal specifieke voorbereidingshandelingen. In algemene zin kan voor de Nederlandse situatie verwezen worden naar de algemene voorbereidingsbepaling van artikel 46 Sr; daar gaat het om de voorbereiding van misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van 8 jaar of meer is gesteld. Die bepaling kan derhalve van betekenis zijn bij die computerdelicten die een hoge maximumstraf kennen, zoals artikel 161sexies, onderdelen 3° en 4°.

Daarnaast kent het huidige artikel 139d de strafbaarstelling van een specifiek soort voorbereidingshandeling die ten deze relevant kan zijn: strafbaar is hij die een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn, met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen. Ook artikel 350a, derde lid, kent een in dit opzicht relevante strafbaarstelling van een voorbereidingshandeling: strafbaar is degene die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk.

Voor het overige dient de Nederlandse strafwet aangevuld te worden met een specifieke bepaling die tegemoet komt aan artikel 6 Verdrag. Daartoe worden aan artikel 139d twee nieuwe artikelleden toegevoegd die aansluiten bij de verdragsbepaling. De verdeling in twee leden heeft betekenis voor de verschillen in strafmaat. Indien het oogmerk is gericht op een misdrijf als bedoeld in artikel 138a, eerste lid (eenvoudige computervredebreuk), 138b (belemmering van de functie van een computer) of 139c (aftappen of opnemen van computergegevens), wordt de strafmaat – zoals hiervoor in deze toelichting reeds aangegeven – bepaald op een jaar. Indien het oogmerk gericht is op een misdrijf als bedoeld in artikel 138a, tweede of derde lid, wordt aangesloten bij de voor die delicten zelf bedreigde maximumstraf, d.w.z. vier jaar. Degene die een instrument vervaardigt of verkoopt met specifiek het oogmerk dat daarmee het gekwalificeerde delict van artikel 138a, tweede of derde lid, wordt gepleegd, dient ook zelf te worden bedreigd met de daarbij passende hogere maximumstraf.

Het tweede lid van artikel 6 Verdrag bepaalt uitdrukkelijk dat artikel 6 niet zodanig mag worden geïnterpreteerd dat strafbaar moet worden gesteld het gedrag waarbij niet de bedoeling voorzit om een strafbaar feit te plegen. Dit is naar Nederlands recht afgedekt door in de delictsbepaling het «oogmerk» op te nemen. Indien iemand een technisch hulpmiddel voorhanden heeft dat hoofdzakelijk ontworpen is tot het plegen van computervredebreuk (138a Sr) maar hij dit hulpmiddel alleen gebruikt om de beveiliging van z'n eigen computer te testen, heeft hij niet het oogmerk om het misdrijf computervredebreuk te plegen. Hij valt dan dus niet in de termen van de strafbepaling.

In het oorspronkelijke voorstel van wet «computercriminaliteit II» werd het eerste lid van artikel 139d reeds gewijzigd terzake van het begrip «gegevensoverdracht». Deze wijziging is in de bijgaande nota van wijziging verwerkt.

8. (Nieuw onderdeel Ia ter vervanging van (gedeelte) onderdeel I wetsvoorstel inzake artikel 139e Sr)

In het oorspronkelijke wetsvoorstel waren de wijzigingen van artikel 139d en artikel 139e in één onderdeel samengevoegd. Doordat de wijziging van artikel 139d wordt uitgebreid, wordt de wijziging van artikel 139e als apart onderdeel opgenomen. Inhoudelijk is geen sprake van een wijziging ten opzichte van het oorspronkelijke wetsvoorstel.

9. (Onderdeel J wetsvoorstel, inzake aanvulling artikel 161sexies Sr; betreft artikel 6 Verdrag)

Op dezelfde wijze als artikel 139d wordt aangevuld met bepalingen inzake de strafbaarstelling van de voorbereiding van strafbare feiten als bedoeld in de artikelen 138a, 138b en 139c, wordt artikel 161sexies aangevuld met een bepaling inzake de strafbaarstelling van de voorbereiding van een strafbaar feit als bedoeld in dat artikel. Zoals in paragraaf 3.1 aangegeven, wordt de maximumstraf in het eerste lid verhoogd van zes maanden naar een jaar en wordt de maximumstraf in het nieuwe tweede lid eveneens op een jaar gesteld.

In de oorspronkelijke tekst van het voorstel van wet werd artikel 161sexies reeds in redactioneel opzicht gewijzigd. In de bijgaande nota van wijziging is die redactionele wijziging geïncorporeerd.

10. (Nieuw onderdeel Ja ter vervanging van (gedeelte) onderdeel J wetsvoorstel, inzake artikel 161septies Sr)

In het oorspronkelijke wetsvoorstel waren de wijzigingen van artikel 161sexies en artikel 161septies in één onderdeel samengevoegd. Doordat de wijziging van artikel 161sexies wordt uitgebreid, wordt de wijziging van artikel 161septies als apart onderdeel opgenomen. Inhoudelijk is geen sprake van een wijziging ten opzichte van het oorspronkelijke wetsvoorstel.

11. (Onderdeel K wetsvoorstel, inzake artikel 232 Sr)

De tekst van het tweede lid van artikel 232 Sr wordt aangepast aan de wijziging van dat artikel die tot stand is gekomen door de wet van 21 april 2004 tot wijziging van het Wetboek van Strafrecht in verband met de bestrijding van freaude en vervalsing in verband met andere betaalmiddelen dan contanten (fraude niet-chartaal geldverkeer) (Stb. 180). Daardoor kan ook artikel II van die wet vervallen, dat strekte tot wijziging van het onderhavige onderdeel K (zie hierna de toelichting op nummer 28 van deze nota van wijziging).

12. (Onderdeel L wetsvoorstel, inzake artikel 273d Sr)

Naar aanleiding van het advies van het CBP om de reikwijdte van de strafbaarstelling van schending van het telefoongeheim te verruimen naar de niet-openbare telecommunicatienetwerken endiensten, wordt het in het wetsvoorstel opgenomen artikel 273d Sr – dat in de plaats komt van het huidige artikel 374bis Sr – dienovereenkomstig gewijzigd. Het opzettelijk en wederrechtelijk kennisnemen, overnemen, aftappen of opnemen van gegevens die door tussenkomst van zodanige netwerken of diensten worden verwerkt of overgedragen en die niet voor betrokkene

bestemd zijn, wordt hiermee strafbaar. Zoals het CBP terecht opmerkt zijn inbreuken op communicatie middels niet-openbare netwerken veelal niet strafbaar indien deze worden gepleegd door de rechthebbende op het netwerk. De door het CBP aan de orde gestelde vraag of niet ook aan de toegang van de rechthebbende tot communicatie over zijn eigen netwerk nadere voorwaarden dienen te worden gesteld ter bescherming van het telecommunicatiegeheim van de gebruikers van dat netwerk, beantwoord ik bevestigend. Zeker voor omvangrijke private netwerken waarin vele duizenden personen plegen te communiceren in verschillende posities en onderlinge verhoudingen en met uiteenlopende redelijke verwachtingen ten aanzien van de bescherming van de vertrouwelijkheid van de communicatie, acht ook ik nadere voorwaarden wenselijk. Dergelijke voorwaarden zullen van belang kunnen zijn bij de beoordeling van de vraag in hoeverre het handelen van de rechthebbende op het netwerk – veelal de werkgever – als wederrechtelijk moet worden beschouwd, c.q. onder welke omstandigheden de gegevens mede bestemd moeten worden geacht voor die rechthebbende.

Onder verantwoordelijkheid van het CBP zijn vuistregels ontwikkeld voor controle op e-mail en internetgebruik van werknemers («*Goed werken in netwerken. Regels voor controle op e-mail en internetgebruik door werknemers*». College bescherming persoonsgegevens, april 2002. Achtergronden en Verkenningen 21). Controle van e-mail is op zichzelf niet verboden. De werkgever is bevoegd om op basis van zijn gezagsbevoegdheid voorwaarden te stellen aan het gebruik van e-mailfaciliteiten of bepaalde soorten gebruik te verbieden. De werkgever zal de doeleinden moeten bepalen waarvoor hij controle noodzakelijk acht. De maatregelen zullen in redelijke verhouding moeten staan tot de belangen van de werknemer. Dit geldt ook voor de controle op het internetgebruik door werknemers. Om de toepasbaarheid van de vuistregels te vergroten, heeft het CBP een raamregeling voor het gebruik van e-mail en internetgebruik ontwikkeld, bedoeld als instrument waarmee organisaties de vuistregels kunnen vertalen naar het eigen beleid. De concrete invulling van het beleid is maatwerk en dient in overleg tussen werkgever en werknemers (bijvoorbeeld de ondernemingsraad) tot stand te komen. Daarbij kan bijvoorbeeld vastgelegd worden dat controle in beginsel alleen plaatsvindt op het niveau van getotaliseerde gegevens, en dat tot controle op individueel niveau kan worden overgegaan indien het vermoeden bestaat dat een werknemer of groep van werknemers de regels overtreedt. De controle op e-mail en internetgebruik zal in beginsel moeten worden uitgevoerd overeenkomstig de terzake gemaakte afspraken of het terzake vastgestelde beleid. Het kennisnemen van gegevens door de werkgever zal in dat geval in beginsel niet als wederrechtelijk kunnen worden aangemerkt.

De uitbreiding van de werkingssfeer van de strafbepaling tot de niet-openbare telecommunicatienetwerken en -diensten wordt vormgegeven door een apart tweede lid bij het voorgestelde artikel 273d Sr, zodat deze uitbreiding op een zodanig tijdstip in werking kan treden dat men zich daarop afdoende heeft kunnen voorbereiden.

13 en 14. (Onderdelen N en O wetsvoorstel, inzake de artikelen 350a en 350b Sr)

In de oorspronkelijke tekst van het wetsvoorstel werd in artikel 350a Sr geschrapt «dan wel andere gegevens daaraan toevoegt» en in artikel 350b de zinsnede «dan wel dat andere gegevens daaraan worden toegevoegd», omdat deze zinsnedes geen toegevoegde waarde hadden naast de termen veranderen, wissen etcetera. Bij nadere overweging meen ik evenwel dat deze zinsnedes wel degelijk toegevoegde waarde hebben, bijvoorbeeld met het oog op de strafbaarheid van het opzettelijk en wederrechtelijk (bijvoorbeeld zonder toestemming van de geadresseerde) meezenden van

(verborgen) gegevens over de e-mail. Daarom stel ik voor de bedoelde zinsnedes te handhaven.

15.

De aanhef van de wijziging van het Wetboek van Strafvordering wordt up to date gemaakt. Een aantal van de in het Wetboek van Strafvordering voorgestelde wijzigingen heeft betrekking op artikelen die ook in ander verband onderhevig zijn aan wetswijziging; dat speelt vooral een rol in de bepalingen van de zevende en achtste afdeling van titel IVa van het Wetboek van Strafvordering. Voor de overzichtelijkheid is daarom in bijlage II een doorlopende tekst opgenomen van de bedoelde artikelen zoals deze zouden komen te luiden na verwerking van de daarbij vermelde wetswijzigingen.

16. (Nieuw onderdeel A, inzake wijziging van artikel 67 Sv; betreft artikel 14 Verdrag)

Op deze wijziging van artikel 67 Sv ben ik in paragraaf 2.2 van deze toelichting reeds kort ingegaan naar aanleiding van het advies van het OM.

Artikel 14 van het Verdrag verplicht de verdragspartijen ertoe dat zij de specifieke opsporingsbevoegdheden van afdeling 2 toepasselijk maken ten aanzien van (a) de strafbare feiten die in de artikelen 1 tot en met 11 van het Verdrag zijn omschreven, (b) andere door middel van een computersysteem begane strafbare feiten en (c) de vergaring van bewijs in elektronische vorm van enig strafbaar feit. Deze verplichting verdient evenwel enige nuancering in het licht van artikel 15 van het Verdrag.

In het algemeen is het gebruikelijk om in de wet te bepalen wanneer een bepaalde bevoegdheid toepassing kan vinden en met welke waarborgen de toepassing ervan is omgeven ter bescherming van de rechten van de verdachte en van derden, zoals bijvoorbeeld neergelegd in het EVRM. De wijze waarop deze bescherming in nationale wettelijke stelsels wordt vormgegeven, is zeer divers. Het invoeren van min of meer geharmoniseerde voorwaarden en waarborgen met betrekking tot de bepalingen van afdeling 2, zou gemakkelijk kunnen leiden tot discrepanties en daarmee tot onduidelijkheden en onvolkomenheden in de nationale wettelijke stelsels. Dit geldt des te meer voor die verdragspartijen die geen partij zijn bij het EVRM, maar wel bij andere verdragen ter bescherming van fundamentele rechten. Het verdrag laat het daarom aan de verdragspartijen over om voorwaarden en waarborgen toe te passen op de bevoegdheden van afdeling 2 zoals deze onder het nationale recht gebruikelijk zijn en die het beste aansluiten bij de nationale wetgevingstraditie. Het ligt daarbij voor de hand om aan te sluiten bij de voorwaarden en waarborgen die gelden voor overeenkomstige of verbonden bevoegdheden. Artikel 15 noemt in het tweede lid een aantal voorbeelden van dergelijke mogelijke voorwaarden en waarborgen, zoals controle door de rechter, het formuleren van toepassingsvoorwaarden, het beperken van het toepassingsgebied of het beperken van de toepassingsduur.

Hoewel het een verdragspartij niet vrijstaat te bepalen welke van de in het verdrag opgenomen bevoegdheden zij in haar wetgeving opneemt, staat het haar derhalve wel vrij om de modaliteiten van deze bevoegdheden te bepalen, voor zover dat nodig is in het licht van de fundamentele rechten en belangen en de uitwerking daarvan. Een en ander is uiteengezet in het *Explanatory Memorandum* bij het Verdrag, in het bijzonder paragraaf 145.

De bevoegdheden waarvan hier sprake is worden naar Nederlands recht doorgaans slechts mogelijk gemaakt voor feiten waarvoor op de voet van artikel 67, eerste lid, van het Wetboek van Strafvordering voorlopige hechtenis is toegelaten. Dat zijn in ieder geval de feiten waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld (onderdeel a) en daarnaast enkele bijzondere feiten, omschreven in artikel 67, eerste lid, onderdelen b en c, Strafvordering.

De computerdelicten zoals deze thans reeds deel uitmaken van het Nederlandse Wetboek van Strafrecht en zoals zij ter implementatie van het Verdrag worden gewijzigd of aangevuld, vallen onder de categorie van artikel 67, eerste lid, onderdeel a, voor zover voor deze delicten een maximum strafmaat van vier jaren gevangenisstraf of meer is voorzien. In de Nederlandse traditie zou dit betekenen dat de toepassing van de dwangmiddelen zoals omschreven in het verdrag niet mogelijk is voor delicten die niet als ernstig in de zin van art. 67 eerste lid, onderdeel a, zijn aangemerkt, of die niet in de opsomming in de onderdelen b en c van hetzelfde artikel zijn opgenomen. Een dergelijke beperking van het toepassingsbereik van de bevoegdheden van sectie 2 van het verdrag zou, hoewel strikt genomen wellicht verdedigbaar, naar mijn mening in strijd zijn met de ratio van het Verdrag. Vanwege de aard van de gedragingen en de technische omgeving waarin deze delicten worden gepleegd, dienen de specifieke bevoegdheden van het verdrag toegepast te kunnen worden ter opsporing van strafbare feiten zoals beschreven in de artikelen 138a, 138b, 139c, 139d, tweede lid, 350a en 350b Sr.

Aan de andere kant voorziet het Nederlandse Wetboek van Strafvordering, met inachtneming van de toepasselijke verdragen, in een stelsel waarbij zwaardere waarborgen gelden naarmate sprake is van ingrijpender bevoegdheden. De enkele toevoeging van specifieke computerdelicten aan artikel 67 Sv leidt er dan ook niet toe dat alle in het Verdrag voorziene bevoegdheden ook te allen tijde voor de opsporing daarvan kunnen worden ingezet. Juist waar het gaat om bevoegdheden die een aanzienlijke inbreuk kunnen betekenen op de persoonlijke levenssfeer, dient de inzet daarvan genormeerd te zijn. Deze normering ligt besloten in de specifieke wetsbepalingen waarin de bevoegdheden geregeld zijn. Als voorbeeld wijs ik op artikel 126m Sv: de daarin geregelde bevoegdheid tot het opnemen van telecommunicatie kan slechts toegepast worden in geval van verdenking van een misdrijf als bedoeld in artikel 67, eerste lid, Sv, maar daarbij geldt tevens de beperking dat het moet gaan om een misdrijf dat in concreto – gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven – een ernstige inbreuk op de rechtsorde oplevert. Bovendien is de officier van justitie slechts bevoegd na een schriftelijke machtiging van de rechter-commissaris.

17, 17a en 18. (Vervallen van onderdelen B en D en van grote delen van onderdeel E van het wetsvoorstel; opneming van nieuwe onderdelen B en D)

De (bestaande) onderdelen B en D van het wetsvoorstel en de in onderdeel E voorgestelde nieuwe artikelen 125n, 125p en 125q kunnen vervallen omdat in de daarmee geregelde materie inmiddels in breder verband wordt voorzien door het eerdergenoemde voorstel van wet inzake bevoegdheden vorderen gegevens (Kamerstukken II 2003/04, 29 441).

In verband met dat wetsvoorstel zijn nog wel enkele technische aanpassingen nodig, die worden opgenomen in de (nieuwe) onderdelen B en D.

In het nieuwe onderdeel B (wijziging van artikel 125k Sv) wordt een omissie hersteld die was ontstaan doordat in wetsvoorstel 29 441 het oude artikel 125m geheel was vervallen, terwijl enkele elementen hadden

moeten worden gehandhaafd. Deze elementen worden als derde lid toegevoegd aan artikel 125k Sv.

Het nieuwe onderdeel D (wijziging van artikel 125m Sv) strekt ertoe dat de zogenaamde notificatieplicht – door wetsvoorstel 29 441 voor de situatie waarin gegevens worden «vastgelegd» opgenomen in artikel 125m, eerste lid, Sv – ook van toepassing is in de situatie waarin gegevens door toepassing van het voorgestelde artikel 125o worden «ontoegankelijk gemaakt».

19. (Artikelen 126la, 126m en 126ma Sv)

Zoals in de paragrafen 2.5 en 3.1.1 van deze toelichting, mede naar aanleiding van het advies van het OM, al aan de orde kwam, is het wenselijk om in artikel 126m uitdrukkelijk tot uiting te brengen dat het opnemen van telecommunicatie met een technisch hulpmiddel zowel met als zonder medewerking van de aanbieder kan plaatsvinden; het Verdrag verplicht daar ook toe. Daarnaast verplicht het Verdrag ertoe de bevoegdheid te creëren om communicatie op te nemen die plaatsvindt met gebruikmaking van de diensten van een serviceprovider in de zin van het Verdrag, dat wil zeggen degene die aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst. Daartoe wordt de werking van artikel 126m uitgebreid tot die categorie van dienstverleners, welke wordt gedefinieerd in het nieuwe artikel 126la. Voor de formulering is nauw aangesloten bij de tekst van het Verdrag. Verreweg de belangrijkste categorie aanbieders die hieronder vallen, betreft de openbare telecommunicatiesector. Maar daarnaast vallen ook de besloten netwerken en diensten onder de begripsbepaling, alsmede diegenen die gegevens verwerken of opslaan ten behoeve van een communicatiedienst of diens gebruikers. Waar artikel 1, sub c, van het Verdrag spreekt over «iedere publieke of private instelling» wordt dit in artikel 126la Sv vertaald als de natuurlijke of rechtspersoon die handelt in de uitoefening van een beroep of bedrijf. Daarmee wordt dezelfde afgrenzing bereikt als met het Verdrag is beoogd. Bijvoorbeeld, de persoon die thuis van zijn computer een webserver maakt en familieleden in de gelegenheid stelt daarop hun websites te plaatsen, valt daarmee niet onder het begrip service provider.

Bij de huidige stand van zaken wordt communicatie op de voet van artikel 126m Sv opgenomen met medewerking van de telecomaanbieders door middel van de zgn. tapkamers. Of het ook mogelijk is communicatie op te nemen zonder de medewerking van de aanbieder, en in het bijzonder communicatie die plaatsvindt binnen besloten netwerken, hangt af van de technische mogelijkheden die de opsporingsautoriteiten ten dienste staan. Aangezien het daarbij echter gaat om een grote inbreuk op de persoonlijke levenssfeer, en gelet op de verschillende methoden die hierbij denkbaar zijn, acht ik het wenselijk dat strenge eisen worden gesteld aan de inzet van deze mogelijkheid. Deze eisen betreffen in ieder geval de zorgvuldige en controleerbare toepassing van de technische hulpmiddelen. In paragraaf 3.1.2 ben ik uitgebreid ingegaan op de opgenomen waarborgen, waaronder de eis dat de technische hulpmiddelen pas mogen worden ingezet als deze voldoen aan de daartoe bij algemene maatregel van bestuur te stellen eisen.

Artikel 126m wordt derhalve aanmerkelijk gewijzigd. In het tweede lid wordt in onderdeel e de eis toegevoegd dat in het bevel de aard moet worden aangeduid van het technisch hulpmiddel waarmee de communicatie zal worden opgenomen. In samenhang hiermee moet de wijziging van artikel 126ee Sv (zie nr. 22, nieuw onderdeel lh) worden bezien: het

technisch hulpmiddel moet voldoen aan daartoe bij algemene maatregel van bestuur te stellen eisen.

In het derde lid wordt als hoofdregel opgenomen dat – als het bevel betrekking heeft op communicatie die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst – het opnemen plaatsvindt met medewerking van de aanbieder. Maar daarbij wordt uitdrukkelijk de mogelijkheid opengehouden dat het opnemen plaatsvindt zonder de medewerking van de aanbieder, namelijk indien dat niet mogelijk is of omdat het belang van strafvordering zich daartegen verzet. Van deze afweging zal vanzelfsprekend proces-verbaal worden opgemaakt. Naar aanleiding van het advies van de NVvR merk ik op dat, indien de medewerking van de aanbieder wordt ingeroepen, deze vanzelfsprekend slechts die gegevens krijgt die noodzakelijk zijn om aan het bevel uitvoering te geven. Het bevel als zodanig is niet gericht tot de aanbieder maar tot de opsporingsambtenaar. De aanbieder heeft te maken met de tot hem gerichte vordering van de officier van justitie, waarin alleen de voor hem noodzakelijke gegevens vermeld zijn. In het derde lid wordt uitdrukkelijk vermeld dat het bevel «vergezeld gaat van» de vordering, zodat duidelijk is dat bevel en vordering niet hetzelfde zijn. Ik wijs er tenslotte op dat op grond van het negende lid (zie hierna) regels kunnen worden gesteld over de bevelen en de vorderingen.

In het vierde lid wordt bepaald dat als het bevel betrekking heeft op andere communicatie (bijvoorbeeld in private netwerken), de aanbieder van de betrokken dienst in ieder geval in de gelegenheid moet worden gesteld zijn medewerking daaraan te verlenen. Anders dan bij de openbare telecommunicatiediensten en -netwerken, die op grond van de Telecommunicatiewet een aftapverplichting en een medewerkingsverplichting hebben, wordt in dit geval de medewerking niet gevorderd, maar kan wel de vrijwillige medewerking worden ingeroepen. Het Verdrag houdt in artikel 21 rekening met deze mogelijkheid, waar de verplichte medewerking door serviceproviders slechts hoeft te worden geregeld voor zover dat mogelijk is binnen de bestaande technische mogelijkheden. Voor de aanbieders in de openbare telecommunicatiesector kan er, in aansluiting op de in de Telecommunicatiewet geregelde aftap- en medewerkingsplicht, vanuit worden gegaan dat de technische mogelijkheden er wel zijn, terwijl dat voor de andere aanbieders niet het geval is. De strekking van artikel 21 is bovendien dat zoveel mogelijk wordt zekergesteld dat er een bevoegdheid is om gegevens te vergaren. Daartoe voldoet de voorgestelde regeling. Door in de wet vast te leggen dat de aanbieder in de gelegenheid wordt gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel, wordt vastgesteld dat de aanbieder niet onrechtmatig handelt indien hij aan de opsporingsautoriteiten de gevraagde – vrijwillige – medewerking verleent. Maar ook hier geldt dat de medewerking niet gevraagd hoeft te worden indien deze medewerking niet mogelijk is of het belang van strafvordering zich daartegen verzet. In dat geval zal het bevel ten uitvoer moeten worden gelegd zonder medewerking van de aanbieder.

In het oorspronkelijke wetsvoorstel werden enkele leden toegevoegd aan artikel 126m terzake van kort gezegd de medewerking aan ontsleuteling van telecommunicatie. Deze nieuwe artikelleden zijn in de nieuw geformuleerde bepaling ook weer opgenomen.

Het negende lid betreft de bevoegdheid om bij algemene maatregel van bestuur regels te stellen over de gang van zaken bij bevelen en vorderingen. Het kan daarbij gaan over de wijze waarop de bevelen en vorderingen worden afgegeven, over de inhoud en het «format» van de

bevelen en vorderingen, over de wijze waarop de bevelen worden nagekomen en de vorderingen opgevolgd en dergelijke. Denkbaar is dat hierbij bijvoorbeeld ook regels worden gesteld over de reikwijdte van het bevel indien de gebruiker van de communicatiedienst van nummer wisselt. De algemene maatregel van bestuur zal tot stand komen na overleg met de aanbieders.

In artikel 126m Sv zijn ook enkele artikelleden aangebracht door de wet van 18 maart 2004 houdende enkele wijzigingen in o.m. het Wetboek van Strafvordering betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de Europese Unie (Stb. 2004, 107). Deze artikelleden worden thans ondergebracht in een eigen artikel 126ma.

20. (Ga: wijziging van artikel 126n; Gb, Gc en Gd: wijziging van de artikelen 126na, 126nb en 126ng; Ge: nieuw artikel 126ni)

Ga (wijziging van artikel 126n Sv; betreft artikel 20 Verdrag, voor zover betrekking hebbend op private netwerken)

Artikel 20 van het Verdrag betreft de vastlegging in «real-time» van verkeersgegevens. Verreweg de belangrijkste methode daartoe is het inroepen van de medewerking van de betrokken service provider. Daarover handelt onderdeel b van artikel 20, eerste lid, van het Verdrag. Deze materie valt naar Nederlands recht voor de openbare telecommunicatiesector onder de werking van het huidige artikel 126n Sv (vordering aan aanbieder openbaar telecommunicatienetwerk of – dienst om gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer mbt die gebruiker). Het verdragsartikel strekt zich echter, gelet op de betekenis van het begrip service provider in artikel 1 van het Verdrag, niet alleen uit tot de openbare telecomsector maar ook daarbuiten.

Ons wettelijk stelsel voorziet door middel van artikel 126n van het Wetboek van Strafvordering in de bevoegdheid van de officier van justitie om van de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst te vorderen, dat deze bepaalde gegevens verstrekt over een gebruiker en over het telecommunicatieverkeer met betrekking tot die gebruiker, de verkeersgegevens. De wetgeving voorziet jegens andere entiteiten die onder het ruime verdragsbegrip «service provider» vallen, niet in een dergelijke specifieke vordering. Strikt genomen zou gebruik kunnen worden gemaakt van de nieuwe, in het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441) voorgestelde artikelen 126nd en 126ne Sv. Die artikelen betreffen de bevoegdheid van de officier van justitie om van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, te vorderen deze gegevens te verstrekken. De bevoegdheid kan zich mede uitstrekken tot gegevens die eerst na het tijdstip van de vordering worden verwerkt en ten aanzien waarvan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, kan bepalen dat de gegevens direct na de verwerking worden verstrekt. Ik geef er echter de voorkeur aan, de vordering van verkeersgegevens voor besloten telecommunicatienetwerken en -diensten specifiek te regelen in het kader van artikel 126n Sv, in aansluiting op de regeling voor de openbare telecomsector. Daartoe wordt in het gewijzigde eerste lid van artikel 126n aangesloten bij het begrip «communicatiedienst» dat ook in artikel 126m wordt gehanteerd en dat is gedefinieerd in het nieuwe artikel 126la. Welke gegevens daadwerkelijk onder het bereik van artikel 126n Sv vallen, wordt vastgesteld bij algemene maatregel van bestuur.

Gb, Gc en Gd (wijziging van de artikelen 126na, 126nb en 126ng)

De artikelen 126na en 126nb, zoals voorgesteld in het wetsvoorstel

inzake bevoegdheden vorderen gegevens (29 441), worden aangepast aan de hiervoor toegelichte wijzigingen in het Wetboek van Strafvordering.

In artikel 126ng, zoals voorgesteld in genoemd wetsvoorstel, wordt bepaald dat een vordering als bedoeld in de artikelen 126nc, 126nd en 126ne, slechts tot de aanbieder van een openbare telecommunicatiedienst c.q. openbaar telecommunicatienetwerk kan worden gericht, voor zover de artikelen 126n en 126na geen soelaas bieden. Voor andere entiteiten kon een vordering als bedoeld in de artikelen 126nc, 126nd en 126ne worden gericht, dus ook voor diegenen die onder het ruimere begrip «serviceprovider» van het Verdrag vallen maar geen aanbieder van een openbare telecommunicatiedienst c.q. openbaar telecommunicatie-netwerk zijn. Maar nu ik voorstel artikel 126n voortaan ook toe te passen ten opzichte van de ruimere groep aanbieders van communicatiediensten in de zin van artikel 126la-nieuw Sv, moet de afgrenzingsbepaling van artikel 126ng dienovereenkomstig worden aangepast. Hiermee is tevens toegelicht dat ten opzichte van de besloten telecommunicatienetwerken en -diensten niet zozeer sprake is van een nieuwe bevoegdheid – deze was immers met het wetsvoorstel inzake bevoegdheden vorderen gegevens (29 441) reeds geïntroduceerd – als wel van een andere – meer specifieke – bevoegdheids*grondslag*.

Ge (nieuw artikel 126ni Sv; betreft artikelen 16 en 17 Verdrag inzake bevriezing computergegevens en snelle ontsluiting verkeersgegevens)

Artikel 16 van het Verdrag betreft de mogelijkheid om op uiterst korte termijn te vorderen dat specifiek aan te duiden gegevens voor een relatief korte termijn beschikbaar blijven. Het gaat hierbij om zgn. vluchtige gegevens, waarbij het risico bestaat dat deze zonder een dergelijke vordering niet in dezelfde staat bewaard zouden blijven. Uitdrukkelijk zij hierbij meteen aangetekend dat het hier niet gaat om een algemene verplichting om heel in het algemeen gegevens voor een bepaalde termijn vast te leggen, maar om een plicht in een bepaald geval, indien dit nodig is in het belang van het opsporingsonderzoek, gespecificeerde gegevens die zijn opgeslagen, te bewaren en beschikbaar te houden.

Een dergelijke vordering aan de houder van gegevens kan alleen worden gedaan, indien het bij de strafvorderlijke autoriteiten bekend is dat vluchtige gegevens aanwezig kunnen zijn, die nodig zouden kunnen zijn voor het onderzoek. Een voorbeeld waarin dit het geval kan zijn betreft de situatie waarin bij een schietincident met slachtoffers veel mogelijke betrokkenen op de plaats van het incident aanwezig waren en gegevens over deze betrokkenen wellicht beschikbaar zijn omdat zij in de buurt van het incident elektronische handelingen hebben verricht of gebruik van mobiele telecommunicatie hebben gemaakt. Denkbaar is dat de strafvorderlijke autoriteit van de bedrijven die beschikken over deze gegevens vordert gedurende een korte periode deze gegevens beschikbaar te houden, in afwachting van de (met meer waarborgen omklede) beslissing om al of niet de gegevens zelf te vorderen.

De bevoegdheid als voorgesteld in het nieuwe artikel 126ni wordt beperkt tot gevallen waarbij sprake is 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, en dan nog alleen indien het belang van het onderzoek dit dringend vordert. De vordering kan worden gericht tot 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, maar vanzelfsprekend niet tot de verdachte.

Bij de vordering zal moeten worden aangegeven voor welke termijn de gegevens bewaard en beschikbaar gehouden moeten worden. Het Verdrag bepaalt dat een maximumtermijn van 90 dagen nodig is; dat heeft

als reden dat rekening moet worden gehouden met de relatief lange periode die in een aantal landen gemoeid is met de uitvoering van een rechtshulpverzoek. Indien de vordering zou plaatsvinden in het kader van een puur Nederlandse aangelegenheid zal doorgaans een veel kortere periode kunnen volstaan. Gelet op de noodzakelijke proportionaliteit zal de periode dan zo kort mogelijk moeten worden vastgesteld. Van belang bij dit alles blijft te bedenken, dat de enkele vordering om bepaalde gegevens te «bevriezen» minder belastend is voor de privacy van de personen op wie de gegevens betrekking hebben dan de vordering om bepaalde gegevens (direct) te verstrekken.

Indien de houder, ingevolge de regels die gelden voor de omgang met persoonsgegevens, de gegevens gedurende deze periode niet (meer) voor zijn eigen activiteiten mag verwerken, betekent dit dat hij de gegevens apart moet opslaan. Gedurende de periode waarin de houder de gegevens beschikbaar moet houden, dient hij in te staan voor de integriteit van de gegevens. Hij mag met de aldus beschikbaar gehouden gegevens geen verdere of andere verwerking plegen en hij mag onbevoegden geen inzage of kennisneming toestaan. Zodra de specifiek bepaalde periode verstreken is, worden voor de houder de regels die normaliter gelden weer volledig van toepassing. Doorgaans zal dat betekenen dat de aldus beschikbaar gehouden gegevens als zodanig moeten worden vernietigd.

In sommige gevallen is denkbaar dat het verloren gaan van gegevens ook voorkomen kan worden door inbeslagneming van de gegevensdrager. Inbeslagneming kan echter disproportioneel zijn, vooral indien dit grote gevolgen heeft voor de bedrijfsvoering van de houder. Een bevel de gegevens beschikbaar te houden, kan dan minder belastend zijn voor de houder van de gegevens.

De vordering kan alleen worden gedaan met betrekking 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. En de vordering kan alleen worden gericht tot degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot die bepaalde gegevens. Daarbij geldt vanzelfsprekend dat geen onevenredige inspanning mag worden verlangd van degene tot wie de vordering wordt gericht.

Het OM heeft geadviseerd in het artikel de terminologie «bewaren en beschikbaar houden» te hanteren. Aan dit advies is tegemoet gekomen.

Het OM heeft ook nog de vraag opgeworpen of gegevens die worden opgeslagen in de naar hun aard tijdelijke werkgeheugens van computers, moeten worden beschouwd als opgeslagen gegevens in de zin van dit artikel. Deze vraag kan bevestigend worden beantwoord, maar daarbij past wel de aantekening dat de vordering niet tot de verdachte kan worden gericht. Het ligt dan ook, mede gelet op de strekking van de bevoegdheid en de daarbij in acht te nemen waarborgen, niet voor de hand dat de bevoegdheid voor dergelijke gegevensopslag zal worden ingezet.

Artikel 16, derde lid, van het Verdrag bepaalt dat aan degene tot wie de vordering gericht is, geheimhouding moet kunnen worden opgelegd. Dit wordt geregeld door artikel 126bb Sv aan te vullen met een verwijzing naar artikel 126ni; hetzelfde wordt gedaan ten aanzien van artikel 126ui. Verwezen zij naar de toelichting op de wijziging van artikel 126bb Sv hierna.

Artikel 17 van het Verdrag schrijft onder meer voor dat verzekerd wordt dat de vordering om verkeersgegevens beschikbaar te houden effect kan hebben, los van de vraag hoeveel aanbieders betrokken zijn bij de verzending (transmission) van het desbetreffende bericht. Daarnaast moet

verzekerd worden dat de aanbieder aan de bevoegde ambtenaar zo spoedig mogelijk die verkeersgegevens bekendmaakt die nodig zijn om ook aan een andere aanbieder de vordering te doen tot het beschikbaar houden van bepaalde gegevens. Dit wordt geregeld in het tweede lid van het voorgestelde artikel 126ni.

Het Overlegorgaan Post en Telecommunicatie (OPT) heeft in zijn advies in het bijzonder aandacht gegeven aan dit nieuw voorgestelde artikel. Het OPT heeft daarbij aangegeven dat, nu de omvang en reikwijdte van de gegevens waarvan bevriezing kan worden gevorderd niet vooraf kan worden bepaald, (mobiele) telecomoperators kunnen worden geconfronteerd met niet voorzienbare extra investeringen voor extra datacapaciteit; het OPT verzocht aan te geven of en in hoeverre aan deze belangen tegemoet kan worden gekomen.

In het kabinetsstandpunt over het rapport «Gegevens in strafvordering» van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Kamerstukken II 2001/02, 28 366, nr. 1) is aangegeven dat het kabinet instemt met het voorstel van de Commissie om de kosten die aan nakoming van een vordering kunnen worden toegerekend in de vorm van extra personeelskosten en extra administratiekosten voor vergoeding in aanmerking komen voor zover deze kosten inzichtelijk worden gemaakt aan de overheid. Dit sluit aan bij de regeling van artikel 592 van het Wetboek van Strafvordering. Dit artikel regelt de vergoeding van kosten voor de uitlevering of overbrenging van voorwerpen en van het vastleggen of overbrengen van geautomatiseerde gegevens. Het gaat daarbij om de kosten die verbonden zijn aan een individuele vordering of een individueel bevel. Het gaat niet om kosten die in het kader van de reguliere activiteiten toch al worden gemaakt. Overigens ga ik er vanuit dat investeringen niet nodig zullen zijn. In het bijzonder voor de mobiele telecomoperators geldt ingevolge artikel 13.4, tweede lid, van de Telecommunicatiewet al een bewaartermijn van drie maanden voor verkeersgegevens.

Het OPT heeft ook gevraagd, hoe de integriteit van de bevroren gegevens moet worden gewaarborgd, in welk formaat de gegevens beschikbaar gehouden moeten worden en of daarover met de sector afspraken kunnen worden gemaakt. Het ligt inderdaad in de rede dat in algemene zin afspraken worden gemaakt tussen het openbaar ministerie en de desbetreffende branche over de wijze waarop de vordering ten uitvoer moet worden gelegd en – eventueel – over de inspanning die nodig is om vernietiging of aantasting van de gegevens tegen te gaan. Ook in concrete gevallen ligt het voor de hand dat de officier van justitie met degene tot wie de vordering is gericht, overleg pleegt over de wijze waarop de vordering ten uitvoer dient te worden gelegd. De kosten van het nakomen van de vordering worden vergoed op de grondslag van artikel 592 Sv.

Het OPT heeft tenslotte gevraagd of met de onderhavige nieuwe bepaling van artikel 126ni niet een disproportionele inbreuk op de persoonlijke levenssfeer van mobiele bellers wordt gemaakt. Het OPT noemde als voorbeeld dat wordt besloten tot bevriezing van gegevens in een bepaalde GSM-cel, waarbij sprake is van een aanzienlijke «bijvang» van gegevens; na de bevriezing zou van een operator – aldus het OPT – gevorderd kunnen worden om de gegevens van een bepaalde gebruiker uit te leveren aan Justitie, waarbij de operator met behulp van datamining uit de bevroren gegevens de gegevens van de gewenste gebruiker zou moeten filteren, terwijl deze verwerking van persoonsgegevens niet «gedekt» wordt door de Wet bescherming persoonsgegevens of een andere wet. In reactie hierop zij erop gewezen dat de onderhavige bevoegdheid louter betreft het niet-vernietigen van gegevens opdat – op een later tijdstip – een vordering kan worden gedaan om bepaalde gegevens te verstrekken. Deze laatste vordering geschiedt alsdan op basis

van een specifieke strafvorderlijke bevoegdheid en dient te voldoen aan de eisen die aan de uitoefening van die bevoegdheid zijn gesteld.

21. (Wijziging artikel 126t)

Artikel 126t wordt op overeenkomstige manier gewijzigd als het equivalent van die bepaling, artikel 126m. Verwezen zij naar de toelichting op onderdeel 19 hierboven, alsmede naar de paragrafen 2.5 en 3.1.1.

22.

Ia (nieuw artikel 126ta)

Het nieuw voorgestelde artikel 126ta is het equivalent van het voorgestelde artikel 126ma. Verwezen zij naar de toelichting op dat nieuwe artikel.

Ib (wijziging 126u Sv; betreft artikel 20 Verdrag, voor zover betrekking hebbend op private netwerken in de situatie bedoeld in 126o Sv)

Op dezelfde wijze als waarop de werking van artikel 126n in verband met het Verdrag moet worden uitgebreid naar private netwerken, dient ook de werking van artikel 126u te worden uitgebreid. Verwezen zij naar de toelichting terzake van artikel 126n.

Ic, Id en Ie (wijziging van de artikelen 126ua, 126ub en 126ug)

Deze wijzigingen zijn het equivalent van de wijzigingen die worden voorgesteld in de artikelen 126na, 126nb en 126ng. Daarnaast wordt van de gelegenheid gebruik gemaakt om in artikel 126ub, laatste volzin, de incorrecte verwijzing naar artikel 126na te vervangen door een juiste verwijzing, namelijk naar artikel 126nb.

If (nieuw artikel 126ui Sv; betreft artikelen 16 en 17 Verdrag inzake bevriezing computergegevens en snelle ontsluiting verkeersgegevens, voor zover van toepassing op de situatie bedoeld in 126o Sv)

Hetgeen in artikel 126ni wordt geregeld voor de situatie waarin sprake is van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, wordt in artikel 126ui synchroon geregeld voor de situatie, bedoeld in artikel 126o: de situatie waarin uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, 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.

Ig (aanvulling 126bb Sv; betreft artikel 16, derde lid, van het Verdrag, voor zover uitgevoerd door de artikelen 126ni en 126ui Sv; betreft tevens artikel 20, derde lid, van het Verdrag, voor zover uitgevoerd door artikel 126n, eerste lid, sub b, en artikel 126u, eerste lid, sub b, Sv)

In enkele bepalingen van het Verdrag wordt uitdrukkelijk vermeld dat geheimhouding moet kunnen worden opgelegd aan degene van wie medewerking wordt gevorderd bij het veiligstellen van gegevens, nl. in artikel 16, derde lid, artikel 20, derde lid, en artikel 21, derde lid. De geheimhouding wordt in het Wetboek van Strafvordering voor dergelijke gevallen geregeld in artikel 126bb, vijfde lid. In dat artikel wordt bepaald dat degene tot wie een specifieke vordering gericht is, in het belang van het onderzoek geheimhouding in acht neemt omtrent al hetgeen hem

terzake van de vordering bekend is. Het past binnen de gekozen systematiek om de in artikel 126bb, vijfde lid, genoemde wetsartikelen aan te vullen met de artikelen 126n, 126u, 126ni en 126ui.

Ih [aanvulling 126ee Sv)

Artikel 126ee bepaalt dat bij algemene maatregel van bestuur technische eisen worden gesteld omtrent de opslag, verstrekking en plaatsing van technische hulpmiddelen. Het betreft thans de hulpmiddelen, bedoeld in de artikelen 126g, derde lid, 126l, eerste lid, 126o, derde lid, en 126s, eerste lid. Zoals hiervoor is uiteengezet is het wenselijk, gelet op de ingrijpendheid van de bevoegdheden, ook technische eisen te stellen aan de technische hulpmiddelen die worden ingezet bij de bevoegdheden inzake het opnemen van telecommunicatie, in het bijzonder indien dit geschiedt zonder medewerking van de aanbieders van (openbare c.q. besloten) netwerken en diensten, zoals voorgesteld in artikel 126m en artikel 126t.

23. (Wijziging artikel 552a Sv)

Mede naar aanleiding van het advies van de Nederlandse Orde van Advocaten merk ik op dat vanzelfsprekend wordt voorzien in een adequate rechtsbescherming. Artikel 552a, eerste lid, van het Wetboek van Strafvordering, dat betrekking heeft op de mogelijkheid van beklag, wordt zowel in het onderhavige wetsvoorstel als in het wetsvoorstel inzake bevoegdheden vorderen gegevens (Kamerstukken II 2003/04, 29 441) gewijzigd. Om beide wijzigingen inéén te schuiven wordt artikel 552a, eerste lid, bij deze nota van wijziging opnieuw geredigeerd waarbij derhalve tevens de elementen zijn verwerkt die afkomstig zijn van het genoemde andere wetsvoorstel. Het onderhavige wetsvoorstel zal naar verwachting immers later in werking treden. De nieuwe, complete formulering van artikel 552a Sv laat zien dat is voorzien in de mogelijkheid van beklag over de vordering van gegevens en over de kennisneming of het gebruik van gegevens, vastgelegd tijdens een doorzoeking of op vordering verstrekt, maar ook over de kennisneming of het gebruik van gegevens, opgeslagen, verwerkt of overgedragen door middel van een geautomatiseerd werk en vastgelegd bij een onderzoek in zodanig werk en over de vordering gegevens te bewaren en beschikbaar te houden.

24. (Wijziging artikel 592a Sv)

Artikel 592, tweede lid, van het Wetboek van Strafvordering betreft de mogelijkheid van vergoeding van de kosten van het nakomen van vorderingen tot – onder andere – het verstrekken van gegevens. Voor de openbare telecommunicatiesector geldt de specifieke regeling van artikel 13.6 van de Telecommunicatiewet. Maar omdat door de uitbreiding van de werking van de artikelen 126m en 126n dergelijke vorderingen in de toekomst ook kunnen worden gericht tot aanbieders die niet onder de werking van de Telecommunicatiewet vallen en aan wie derhalve geen vergoeding op die grondslag kan worden gegeven, dient vergoeding plaats te vinden op de voet van artikel 592 Sv. Waar mogelijk geldt derhalve de specifieke regeling van artikel 13.6 Telecommunicatiewet; in andere gevallen geldt de algemene regeling van artikel 592 Sv.

25. (Wijziging artikel 51a Uitleveringswet)

Artikel 51a van de Uitleveringswet wordt aangevuld met een aanduiding van de misdrijven waarvoor uitlevering mogelijk wordt aan Staten die partij zijn bij het Cybercrime Verdrag. Zoals in dergelijke gevallen gebruikelijk, worden niet alleen de artikelen vermeld die zich naar hun

strekking in hoofdzaak richten op de feiten die door het Verdrag worden bestreken (zoals in dit geval bijvoorbeeld computervredebreuk en het onrechtmatig aftappen van computergegevens) maar ook de artikelen die betrekking hebben op andere delicten die daarbij in beeld kunnen komen (zoals valsheid in geschrifte en vernieling). Vanzelfsprekend wordt de mogelijkheid van uitlevering voor alle feiten beperkt tot de gevallen waarin het desbetreffende feit valt onder de omschrijving van de artikelen 2 tot en met 11 van het Cybercrime Verdrag.

26. (Wijziging artikel III (Telecommunicatiewet))

In aansluiting op het in de Telecommunicatiewet gekozen systeem wordt in artikel 13.2b (dat in de Telecommunicatiewet wordt ingevoegd bij het voorstel van Wet bevoegdheden vorderen gegevens) vastgelegd dat aanbieders van openbare telecommunicatiediensten en -netwerken moeten voldoen aan een vordering als bedoeld in de nieuwe artikelen 126ni en 126ui van het Wetboek van Strafvordering. De aanduiding van de artikelen waarop de verplichting betrekking heeft, wordt derhalve met deze twee artikelen uitgebreid. Artikel 13.2a is inmiddels in de Telecommunicatiewet ingevoegd bij de Wet vorderen gegevens telecommunicatie.

27. (Wijziging van artikel IV, overgangsrecht)

Zoals in de memorie van toelichting is opgemerkt, gelden wat betreft het overgangsrecht in beginsel de hoofdregels, dat wil zeggen ten aanzien van de wijzigingen in de strafbepalingen artikel 1 van het Wetboek van Strafrecht en ten aanzien van de strafvorderlijke bepalingen het beginsel van onmiddellijke werking. Het eerste en tweede lid van de overgangsbepaling kunnen vervallen, zodat een artikellid – het huidige derde lid- overblijft.

Het eerste lid van het in artikel IV van het wetsvoorstel geregelde overgangsrecht kan vervallen omdat de wijziging van artikel 125n Sv uit het wetsvoorstel is verwijderd. Het tweede lid kan vervallen omdat de bevoegdheid waarop het overgangsrecht doelde – het zgn. ontsleutelingsbevel – slechts gehanteerd kan worden «bij of terstond na de toepassing van het eerste lid». Het eerste lid kan worden toegepast zodra de wet in werking is getreden. Doordat de bevoegdheid om een ontsleutelingsbevel te geven, in de tijd zeer strak is gebonden aan de toepassing van dat eerste lid, acht ik overgangsrecht niet nodig.

28.

In artikel II van de wet van 21 april 2004 tot wijziging van het Wetboek van Strafrecht in verband met de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (fraude niet-chartaal geldverkeer) (Stb. 180) is voorzien in een wijziging van het onderhavige wetsvoorstel «computercriminaliteit II». Het betreft een wijziging in artikel 232 Sr. Deze wijziging wordt in het onderhavige wetsvoorstel verwerkt, zodat de overgangsbepaling in eerdergenoemde wet dient te vervallen.

De Minister van Justitie,
J. P. H. Donner

BIJLAGE I

Tekst van de artikelen 139a t/m 139d Wetboek van Strafrecht

Huidige tekst (stand van zaken september 2004):

Artikel 139a

1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met een technisch hulpmiddel een gesprek dat in een woning, besloten lokaal of erf wordt gevoerd opzettelijk:

1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;

2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.

2. Met dezelfde straf wordt gestraft hij die gegevens die in een woning, besloten lokaal of erf, door middel van een geautomatiseerd werk worden overgedragen, met een technisch hulpmiddel opzettelijk, zonder daartoe gerechtigd te zijn, aftapt of opneemt.

3. Het eerste en tweede lid zijn niet van toepassing op het aftappen of opnemen:

1°. van telecommunicatie via een openbaar telecommunicatienetwerk,

2°. behoudens in geval van kennelijk misbruik, met een technisch hulpmiddel dat op gezag van degene bij wie de woning, het lokaal of het erf in gebruik is, niet heimelijk aanwezig is;

3°. ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Artikel 139b

1. Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft hij die, met het oogmerk een gesprek dat elders dan in een woning, besloten lokaal of erf wordt gevoerd af te luisteren of op te nemen, dat gesprek met een technisch hulpmiddel heimelijk:

1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;

2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.

2. Met dezelfde straf wordt gestraft hij die gegevensoverdracht elders dan in een woning, besloten lokaal of erf door middel van een geautomatiseerd werk of telecommunicatie, met een technisch hulpmiddel opzettelijk, zonder daartoe gerechtigd te zijn, heimelijk aftapt of opneemt.

3. Op het eerste en tweede lid is artikel 139a, derde lid, onder 1° en 3°, van overeenkomstige toepassing. Op het tweede lid is artikel 139c, tweede lid, van overeenkomstige toepassing.

Artikel 139c

1. Hij die door middel van een openbaar telecommunicatienetwerk, of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degeen in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

2. Het eerste lid is niet van toepassing op het aftappen of opnemen:

1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.

2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;

3°. ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Artikel 139d

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn.

Tekst zoals deze zou komen te luiden na verwerking van de in Wetsvoorstel CC-II voorgestelde wijzigingen:

Artikel 139a (nieuw)

1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met een technisch hulpmiddel een gesprek dat in een woning, besloten lokaal of erf wordt gevoerd opzettelijk:

1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;

2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.

2. Het eerste lid is niet van toepassing op het opnemen:

1°. van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk,

2°. behoudens in geval van kennelijk misbruik, met een technisch hulpmiddel dat op gezag van degene bij wie de woning, het lokaal of het erf in gebruik is, niet heimelijk aanwezig is;

3°. ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Artikel 139b (nieuw)

1. Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft hij die, met het oogmerk een gesprek dat elders dan in een woning, besloten lokaal of erf wordt gevoerd af te luisteren of op te nemen, dat gesprek met een technisch hulpmiddel heimelijk:

1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;

2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.

2. Artikel 139a, tweede lid, onder 1° en 3°, is van overeenkomstige toepassing.

Artikel 139c (nieuw)

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.

2. Het eerste lid is niet van toepassing op het aftappen of opnemen:

1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.

2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;

3°. ten behoeve van de goede werking van een openbaar

telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Artikel 139d (nieuw)

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn.

2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138a, eerste lid, 138b of 139c wordt gepleegd,

a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of

b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden gekregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

3. Met gevangenisstraf van vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt indien zijn oogmerk is gericht op een misdrijf als bedoeld in artikel 138a, tweede of derde lid.

BIJLAGE II

Tekst van de zevende afdeling van **Titel IV**, de zevende en achtste afdeling van **Titel IVa** en enkele relevante artikelen van **Titel V** en **Titel Vb** van het Wetboek van Strafvordering, zoals deze luiden na verwerking van de wetswijzigingen die voortvloeien uit Stb. 2004, 50 (bezemwet Justitie), Stb. 2004, 105 (vorderen gegevens telecommunicatie), Stb. 2004, 107 (Uitvoeringswet EU-rechtshulpverdrag), Stb. 2004, 109 (vorderen gegevens financiële sector), en Stb. 2004, 577 (Wijziging WvSv ivm inbeslagneming en doorzoeking door de r-c) en met verwerking van de wetswijzigingen die naar verwachting zullen voortvloeien uit wetsvoorstel 29 441 (bevoegdheden vorderen gegevens).

Stand van zaken 15 februari 2005.

NB: hierin is derhalve nog *niet* verwerkt wetsvoorstel 26 671 (computercriminaliteit II).

Titel IV Enige bijzondere dwangmiddelen

(...)

ZEVENDE AFDELING. DOORZOEKING TER VASTLEGGING VAN GEGEVENS

Artikel 125i

Aan de rechter-commissaris, de officier van justitie, de hulpofficier van justitie en de opsporingsambtenaar komt onder dezelfde voorwaarden als bedoeld in de artikelen 96b, 96c, eerste, tweede en derde lid, 97, eerste tot en met vierde lid, en 110, eerste en tweede lid, de bevoegdheid tot tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd. In het belang van het onderzoek kunnen zij deze gegevens vastleggen. De artikelen 96, tweede lid, 98, 99 en 99a zijn van overeenkomstige toepassing.

Artikel 125j

1. In geval van een doorzoeking kan vanaf de plaats waar de doorzoeking plaatsvindt, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar in dat werk opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen, dan kunnen zij worden vastgelegd.
2. Het onderzoek reikt niet verder dan voor zover de personen die plegen te werken of te verblijven op de plaats waar de doorzoeking plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben.

Artikel 125k

1. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij een doorzoeking of bij toepassing van artikel 125j tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel is gericht, dient desgevraagd hieraan gevolg te geven door de kennis omtrent de beveiliging ter beschikking te stellen.
2. Het eerste lid is van overeenkomstige toepassing indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen. Het

bevel richt zich tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens.

Artikel 125l

Naar gegevens die zijn ingevoerd door of vanwege personen met bevoegdheid tot verschoning als bedoeld in artikel 218, vindt, tenzij met hun toestemming, geen onderzoek plaats voor zover daartoe hun plicht tot geheimhouding zich uitstrekt. Een onderzoek in een geautomatiseerd werk waarin zodanige gegevens zijn opgeslagen, vindt, tenzij met hun toestemming, slechts plaats, voor zover dit zonder schending van het stands-, beroeps- of ambtsgeheim kan geschieden.

Artikel 125la

Indien bij een doorzoeking ter vastlegging van gegevens bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst gegevens worden aangetroffen die niet voor deze bestemd of van deze afkomstig zijn, is de officier van justitie slechts bevoegd te bepalen dat van deze gegevens wordt kennisgenomen en dat deze worden vastgelegd, 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, ofwel klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd. De officier van justitie behoeft hiervoor een voorafgaande schriftelijke machtiging, op zijn vordering te verlenen door de rechter-commissaris.

Artikel 125m

1. Leidt een doorzoeking tot vastlegging van gegevens, dan wordt zo spoedig mogelijk aan de betrokkenen schriftelijk mededeling gedaan van deze vastlegging en van de aard van de vastgelegde gegevens. De mededeling blijft achterwege, indien uitreiking van de mededeling redelijkerwijs niet mogelijk is.
2. De officier van justitie dan wel, indien de rechter-commissaris de bevoegdheid tot doorzoeking heeft toegepast, de rechter-commissaris kan bepalen dat de in het eerste lid bedoelde mededeling aan een betrokkene wordt uitgesteld zolang het belang van het onderzoek zich tegen mededeling aan deze betrokkene verzet.
3. Als betrokkene in de zin van dit artikel wordt aangemerkt:
a. de verdachte;
b. de verantwoordelijke voor de gegevens;
c. de rechthebbende van een plaats waar een doorzoeking heeft plaatsgevonden.
4. Indien de betrokkene de verdachte is, kan mededeling achterwege blijven, indien hij door opneming in de processtukken van de vastlegging van gegevens en van de aard van de vastgelegde gegevens op de hoogte komt.

Artikel 125n

1. Zodra blijkt dat de gegevens die zijn vastgelegd tijdens een doorzoeking, van geen betekenis zijn voor het onderzoek, worden zij vernietigd.
2. De vernietiging vindt plaats door of op last van degeen die de gegevens heeft opgenomen. Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt toegevoegd aan de processtukken.
3. De officier van justitie kan bepalen dat gegevens, vastgelegd tijdens een doorzoeking, kunnen worden gebruikt voor:

a. een ander strafrechtelijk onderzoek dan waartoe de bevoegdheid is uitgeoefend;
b. opslag in een register zware criminaliteit, indien het gegevens betreft omtrent een persoon als bedoeld in artikel 13a, eerste lid, onderdeel a tot en met c, van de Wet politieregisters.

4. Indien toepassing is gegeven aan het derde lid, onderdeel a, behoeven de gegevens, in afwijking van het eerste lid, niet te worden vernietigd totdat het andere onderzoek is geëindigd. Is toepassing gegeven aan het derde lid, onderdeel b, dan behoeven de gegevens niet te worden vernietigd, totdat de Wet politieregisters opslag van de gegevens niet meer toestaat.

Titel IVA Bijzondere bevoegdheden tot opsporing

(...)

ZEVENDE AFDELING. ONDERZOEK VAN TELECOMMUNICATIE

Artikel 126m

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 onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar telecommunicatie opneemt met een technisch hulpmiddel.

2. Onder telecommunicatie wordt in dit artikel verstaan niet voor het publiek bestemde communicatie via een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten.

3. Het bevel tot het opnemen van telecommunicatie is schriftelijk en vermeldt:
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, zijn vervuld;
c. het nummer waarmee de individuele gebruiker van telecommunicatie wordt geïdentificeerd, alsmede, voor zover bekend, de naam en het adres van de gebruiker;
d. de geldigheidsduur van het bevel.

4. Indien bij de afgifte van het bevel, bedoeld in het eerste lid, bekend is dat de gebruiker van het nummer, bedoeld in het derde lid, onderdeel c, zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het voornemen tot het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven voordat het bevel ten uitvoer wordt gelegd.

5. Indien na aanvang van het opnemen van de telecommunicatie op grond van een bevel als bedoeld in het eerste lid bekend wordt dat de gebruiker zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven.

6. De officier van justitie kan een bevel als bedoeld in het eerste lid eveneens geven, indien het bestaan van het bevel noodzakelijk is om een andere staat te kunnen verzoeken telecommunicatie met een technisch hulpmiddel op te nemen of telecommunicatie af te tappen en rechtstreeks naar Nederland door te geleiden ter fine van opname met een technisch hulpmiddel in Nederland.

7. Artikel 126l, vierde tot en met achtste lid, is van overeenkomstige toepassing.

Artikel 126n

1. In geval van 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 gebruiker en het telecommunicatieverkeer 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. Onder een gebruiker van telecommunicatie wordt in dit artikel verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede de natuurlijke persoon of rechtspersoon die daadwerkelijk gebruik maakt van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst.

3. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk iedere aanbieder van een openbare telecommunicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing.

4. 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.

5. De officier van justitie doet van de vordering proces-verbaal opmaken, waarin hij vermeldt:

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.

6. 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.

1. 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 126na

1. In In geval van verdenking van een strafbaar feit 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 telecommunicatie. Artikel 126n, tweede en derde 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 achterhaalt en verstrekt.

3. In geval van een vordering als bedoeld in het eerste of tweede lid is

artikel 126n, vijfde 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 126nb

1. Teneinde toepassing te kunnen geven aan artikel 126m of artikel 126n kan de officier van justitie met inachtneming van artikel 3.10, vierde lid, van de Telecommunicatiewet bevelen dat met behulp van in dat artikel bedoelde apparatuur het nummer waarmee de gebruiker van telecommunicatie kan worden geïdentificeerd, wordt verkregen.

2. Het bevel wordt gegeven aan een ambtenaar als bedoeld in artikel 3.10, vierde lid, onder a, van de Telecommunicatiewet en is schriftelijk. Bij dringende noodzaak kan het bevel mondeling worden gegeven. In dat geval stelt de officier van justitie het bevel binnen drie dagen op schrift.

3. Het bevel wordt gegeven voor een periode van ten hoogste een week en vermeldt:

a. de feiten of omstandigheden waaruit blijkt dat voldaan is aan de voorwaarden voor toepassing van artikel 126m of artikel 126n en

b. de naam of een zo nauwkeurig mogelijke aanduiding van de gebruiker van telecommunicatie van wie het nummer moet worden verkregen.

4. De officier van justitie doet te zijnen overstaan de processen-verbaal of andere voorwerpen, waaraan een gegeven kan worden ontleend dat is verkregen door toepassing van het eerste lid vernietigen indien dat gegeven niet gebruikt wordt voor de toepassing van artikel 126m of artikel 126n.

ACHTSTE AFDELING. VORDEREN VAN GEGEVENS

Artikel 126nc

1. In geval van verdenking van een misdrijf kan de opsporingsambtenaar in het belang van het onderzoek van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, vorderen bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon te verstrekken.

2. Onder identificerende gegevens wordt verstaan:

a. naam, adres, woonplaats en postadres;

b. geboortedatum en geslacht;

c. administratieve kenmerken;

d. in geval van een rechtspersoon, in plaats van de gegevens, bedoeld onder a en b: rechtsvorm en vestigingsplaats.

3. Een vordering als bedoeld in het eerste lid kan niet worden gericht tot de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing. De vordering kan geen betrekking hebben op persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging.

4. Een vordering als bedoeld in het eerste lid is schriftelijk en vermeldt:

a. een aanduiding van de persoon op wiens identificerende gegevens de vordering betrekking heeft;

b. de identificerende gegevens die worden gevorderd;

c. de termijn waarbinnen en de wijze waarop de gegevens dienen te worden verstrekt;

d. de titel van de vordering.

5. Bij dringende noodzaak kan een vordering als bedoeld het eerste lid mondeling worden gegeven. De opsporingsambtenaar stelt de vordering

in dat geval achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.

6. Van de verstrekking van identificerende gegevens maakt de opsporingsambtenaar proces-verbaal op, waarin hij vermeldt:

a. de gegevens, bedoeld in het vierde lid;

b. de verstrekte gegevens;

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

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

7. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de opsporingsambtenaar die de gegevens vordert en de wijze waarop de gegevens worden gevorderd en verstrekt.

Artikel 126nd

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 van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, vorderen deze gegevens te verstrekken.

2. Een vordering als bedoeld in het eerste lid kan niet worden gericht tot de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing. De vordering kan niet betrekking hebben op persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging.

3. Een vordering als bedoeld in het eerste lid is schriftelijk en vermeldt:

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

b. een zo nauwkeurig mogelijke aanduiding van de gegevens die worden gevorderd en de termijn waarbinnen, alsmede de wijze waarop deze dienen te worden verstrekt;

c. de titel van de vordering.

4. Bij dringende noodzaak kan de vordering mondeling worden gegeven. De officier van justitie stelt de vordering in dat geval achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.

5. De officier van justitie doet van de verstrekking van gegevens proces-verbaal opmaken, waarin worden vermeld:

a. de gegevens, bedoeld in het derde lid;

b. de verstrekte gegevens;

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

d. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld; e. de reden waarom de gegevens in het belang van het onderzoek worden gevorderd.

6. In geval van verdenking van een ander strafbaar feit dan bedoeld in het eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering als bedoeld in dat lid doen met voorafgaande schriftelijke machtiging van de rechter-commissaris. De rechter-commissaris verleent de machtiging op vordering van de officier van justitie. Het tweede tot en met vijfde lid zijn van overeenkomstige toepassing.

7. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens worden gevorderd en verstrekt.

Artikel 126ne

1. De officier van justitie kan in het belang van het onderzoek bepalen dat een vordering als bedoeld in artikel 126nd, eerste lid, van degene die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, betrekking kan hebben op gegevens die eerst na het tijdstip van de vordering worden verwerkt. De periode waarover de vordering zich uitstrekt is maximaal vier weken en kan telkens met maximaal vier weken worden verlengd. De officier van justitie vermeldt deze periode in de vordering. Artikel 126nd, tweede tot en met vijfde en zevende lid, is van overeenkomstige toepassing.

2. In een geval als bedoeld in het eerste lid bepaalt de officier van justitie dat de uitvoering van de vordering wordt beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in artikel 126nd, eerste lid. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering doet de officier van justitie proces-verbaal opmaken.

3. Indien het belang van het onderzoek dit dringend vordert, kan de officier van justitie in een geval als bedoeld in het eerste lid in de vordering bepalen dat degene tot wie de vordering is gericht de gegevens direct na de verwerking verstrekt, dan wel telkens binnen een bepaalde periode na de verwerking verstrekt. De officier van justitie behoeft hiervoor een voorafgaande schriftelijke machtiging, op zijn vordering te verlenen door de rechter-commissaris.

Artikel 126nf

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 gegevens als bedoeld in artikel 126nd, tweede lid, derde volzin, deze gegevens vorderen.

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

3. Een vordering als bedoeld in het eerste lid kan slechts worden gedaan na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.

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

Artikel 126ng

1. Een vordering als bedoeld in artikel 126nc, eerste lid, 126nd, eerste lid, of 126ne, eerste lid, kan worden gericht tot de aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk de aanbieder van een openbare telecommunicatiedienst, 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 klaarblij-

kelijk 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 eerste 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.

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

Artikel 126nh

1. De officier van justitie kan, indien het belang van het onderzoek dit vordert, bij of terstond na de toepassing van artikel 126nd, eerste lid, 126ne, eerste of derde lid, of 126nf, eerste lid, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen.

2. Het bevel wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.

Titel V Bijzondere bevoegdheden ter opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband

(...)

Artikel 126t

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar met een technisch hulpmiddel telecommunicatie opneemt ten aanzien waarvan het vermoeden bestaat dat daaraan een persoon deelneemt ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in het georganiseerd verband beramen of plegen van misdrijven.

2. Onder telecommunicatie wordt in dit artikel verstaan niet voor het publiek bestemde communicatie via een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten.

3. Het bevel tot het opnemen van telecommunicatie is schriftelijk en vermeldt:

a. een omschrijving van het georganiseerd verband;

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

c. het nummer waarmee de individuele gebruiker van telecommunicatie wordt geïdentificeerd, alsmede, voor zover bekend, de naam en het adres van de gebruiker;

d. de naam van de persoon, genoemd in het eerste lid, wanneer deze niet de houder is, en

e. de geldigheidsduur van het bevel.

4. Indien bij de afgifte van het bevel, bedoeld in het eerste lid, bekend is dat de gebruiker van het nummer, bedoeld in het derde lid, onderdeel c, zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere

staat van het voornemen tot het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven voordat het bevel ten uitvoer wordt gelegd.

5. De officier van justitie kan een bevel als bedoeld in het eerste lid eveneens geven, indien het bestaan van het bevel noodzakelijk is om een andere staat te kunnen verzoeken telecommuncatie met een technisch hulpmiddel op te nemen of telecommunicatie af te tappen en rechtstreeks naar Nederland door te geleiden ter fine van opname met een technisch hulpmiddel in Nederland.

6. Artikel 126s, vierde tot en met achtste lid, is van overeenkomstige toepassing.

Artikel 126u

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 en het telecommunicatieverkeer 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. Onder een gebruiker van telecommunicatie wordt in dit artikel verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede de natuurlijke persoon of rechtspersoon die daadwerkelijk gebruik maakt van een openbaar telecommunicatie-netwerk of een openbare telecommunicatiedienst.

3. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk iedere aanbieder van een openbare telecommunicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing.

4. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt *[NB: abusievelijk is het woord «de» weggevallen; dit wordt gerepareerd bij nota van wijziging CC-II]* vordering gedaan voor een periode van ten hoogste drie maanden.

5. De officier van justitie doet van de vordering proces-verbaal opmaken, waarin hij vermeldt:

a. een omschrijving van het georganiseerd verband;

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.

6. 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 maakt de officier van justitie proces-verbaal op.

7. 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

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 telecommunicatie. Artikel 126u, tweede en derde lid, is van overeenkomstige 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, vijfde 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 126ub

Teneinde toepassing te kunnen geven aan artikel 126t of artikel 126u kan de officier van justitie met inachtneming van artikel 3.10, vierde lid, van de Telecommunicatiewet bevelen dat met behulp van in dat artikel bedoelde apparatuur het nummer waarmee een gebruiker van telecommunicatie kan worden geïdentificeerd, wordt verkregen. Artikel 126na, tweede tot en met vierde lid, is van overeenkomstige toepassing.

Artikel 126uc

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de opsporingsambtenaar in het belang van het onderzoek van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, vorderen bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon te verstrekken.
2. Artikel 126nc, tweede tot en met vijfde en zevende lid, is van overeenkomstige toepassing.
3. Van de verstrekking van identificerende gegevens maakt de opsporingsambtenaar proces-verbaal op, waarin hij vermeldt:
a. de gegevens, bedoeld in artikel 126nc, vierde lid;
b. de verstrekte gegevens;
c. een omschrijving van het georganiseerd verband;
d. de feiten en omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerst lid, zijn vervuld.

Artikel 126ud

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, vorderen deze gegevens te verstrekken.
2. Artikel 126nd, tweede tot en met vierde en zevende lid, is van overeenkomstige toepassing.
3. De officier van justitie doet van de verstrekking van gegevens proces-verbaal opmaken, waarin worden vermeld:
a. de gegevens, bedoeld in artikel 126nd, derde lid;
b. de verstrekte gegevens;
c. een omschrijving van het georganiseerd verband;
d. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;

e. de reden waarom de gegevens in het belang van het onderzoek worden gevorderd.

Artikel 126ue

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek bepalen dat een vordering als bedoeld in artikel 126ud, eerste lid, betrekking kan hebben op gegevens die eerst na het tijdstip van de vordering worden verwerkt. De periode waarover de vordering zich uitstrekt is maximaal vier weken. De officier van justitie vermeldt deze periode in de vordering. De artikelen 126nd, tweede tot en met vierde lid, en 126ud, derde lid, zijn van overeenkomstige toepassing.
2. In een geavl als bedoeld in het eerste lid bepaalt de officier van justitie dat de uitvoering van de vordering wordt beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in artikel 126ud, eerste lid. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering doet de officier van justitie proces-verbaal opmaken.
3. Indien het belang van het onderzoek dit dringend vordert, kan de officier van justitie in een geval als bedoeld in het eerste lid in de vordering bepalen dat degene tot wie de vordering is gericht de gegevens direct na de verwerking verstrekt, dan wel telkens binnen een bepaalde periode na de verwerking verstrekt. De officier van justitie behoeft hiervoor een voorafgaande schriftelijke machtiging, op zijn vordering te verlenen door de rechter-commissaris.

Artikel 126uf

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 gegevens als bedoeld in artikel 126nd, tweede lid, derde volzin, deze gegevens vorderen.
2. De artikelen 126nf, tweede en derde lid, en 126nd, derde, vierde en zevende lid, zijn van overeenkomstige toepassing.
3. De officier van justitie doet van de verstrekking van gegevens proces-verbaal opmaken, waarin worden vermeld:
a. de gegevens, bedoeld in artikel 126nd, derde lid;
b. de verstrekte gegevens;
c. een omschrijving van het georganiseerde verband;
d. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;
e. de reden waarom de gegevens in het belang van het onderzoek worden gevorderd.

Artikel 126ug

1. Een vordering als bedoeld in artikel 126uc, eerste lid, 126ud, eerste lid, of 126ue, eerste lid, kan worden gericht tot de aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk de aanbieder van een 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 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 eerste 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.

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

Artikel 126uh

1. De officier van justitie kan, indien het belang van het onderzoek dit vordert, bij of terstond na de toepassing van artikel 126ud, eerste lid, 126ue, eerste of derde lid, of 126uf, eerste lid, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen.

2. Het bevel wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.

Titel VB Algemene regels betreffende de bevoegdheden in de titels IVA, V en VA

(...)

Artikel 126bb

1. De officier van justitie doet aan betrokkene schriftelijk mededeling van de uitoefening van de bevoegdheden, genoemd in de titels IVa tot en met Va, zodra het belang van het onderzoek dat toelaat. De mededeling blijft achterwege, indien uitreiking van de mededeling redelijkerwijs niet mogelijk is.

2. Als betrokkenen in de zin van het eerste lid worden aangemerkt:

a. de persoon ten aanzien van wie een van de bevoegdheden van titel IVa, V of Va is uitgeoefend;

b. de gebruiker van telecommunicatie of de technische hulpmiddelen waarmee de communicatie plaatsvindt, bedoeld in de artikelen 126m, derde lid, onderdeel c, en 126t, derde lid, onderdeel c;

c. de rechthebbende van een besloten plaats als bedoeld in de artikelen 126g, tweede lid, 126k, 126l, 126o, tweede lid, 126r en 126s, tweede lid.

3. Indien de betrokkene de verdachte is, kan mededeling achterwege blijven indien hij op grond van artikel 126aa, eerste of vierde lid, met de bevoegdheidstoepassing op de hoogte komt.

4. Het eerste lid is niet van toepassing op de uitoefening van de bevoegdheid, bedoeld in de artikelen 126nc en 126uc.

5. Degene tot wie een vordering als bedoeld in de artikelen 126nc tot en met 126nh en 126uc tot en met 126uh is gericht neemt in het belang van het onderzoek geheimhouding in acht omtrent al hetgeen hem terzake van de vordering bekend is.

(...)