Concept

COMPUTERCRIMINALITEIT II

VOORSTEL VAN WET EN MEMORIE VAN TOELICHTING

Ministerie van Justitie
Directie Wetgeving
januari 1998

Concept

COMPUTERCRIMINALITEIT II

VOORSTEL VAN WET EN MEMORIE VAN TOELICHTING

Ministerie van Justitie
Directie Wetgeving
januari 1998

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

Wij Beatrix, bij de Gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.
Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het wenselijk is om, met het oog op nieuwe ontwikkelingen in de informatietechnologie, het Wetboek van Strafrecht en het Wetboek van Strafvordering te wijzigen, onder andere ten aanzien van de uitings- en verspreidingsdelicten;
Zo is het, dat Wij, de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I

Het Wetboek van Strafrecht wordt als volgt gewijzigd:

A

Artikel 53 komt te luiden:

Artikel 53
1. Bij misdrijven gepleegd door middel van de drukpers of door enig ander middel voor de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift, wordt de tussenpersoon als zodanig niet vervolgd, indien:
a. hij bij de openbaarmaking of verspreiding zijn identiteit heeft bekendgemaakt;
b. de dader bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de tussenpersoon is bekendgemaakt, en
c. de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding.
2. Onder de tussenpersoon, bedoeld in het eerste lid, wordt verstaan: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift afkomstig van derden.

B

Artikel 54 komt te luiden:

Artikel 54
Bij misdrijven gepleegd door middel van de drukpers wordt de drukker als zodanig niet vervolgd, indien:
a. het gedrukte stuk zijn naam en woonplaats vermeldt;
b. de persoon op wiens last het stuk is gedrukt, bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de drukker is bekendgemaakt, en
c. de drukker op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van de openbaarmaking of verspreiding.

C

In artikel 80quinquies vervalt "al dan niet".

D

In artikel 80sexies worden de woorden “op te slaan en te verwerken” vervangen door:
op te slaan, te verwerken en over te dragen.

E

In de artikelen 161sexies, 161septies en 351 vervallen de woorden “voor opslag of verwerking van gegevens”.

F

Artikel 138a wordt als volgt gewijzigd:
1. In het eerste lid wordt na het woord "opzettelijk" ingevoegd het woord “en” en vervallen de woorden “voor de opslag of verwerking van gegevens”.
2. In het derde lid, onderdeel a, wordt het woord “zich” vervangen door:
zichzelf of een ander.

G

Artikel 139b, tweede lid, komt te luiden:

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

H

(vervallen)

I

Artikel 232 wordt als volgt gewijzigd:
1. In het eerste lid worden de woorden “bedoeld voor het verrichten van betalingen langs geautomatiseerde weg” vervangen door:

, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg.

2. In het tweede lid wordt "bedreigd" vervangen door: gestraft.

J

Artikel 350a wordt als volgt gewijzigd:

1. In het eerste lid wordt de zinsnede "Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen" vervangen door:
Hij die opzettelijk en wederrechtelijk in een geautomatiseerd werk gegevens die door middel van dat werk zijn opgeslagen, worden verwerkt of overgedragen.

2. In het derde lid wordt de zinsnede "die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk" vervangen door:
die zijn bestemd om schade aan te richten in een geautomatiseerd werk.

K

Artikel 350b wordt als volgt gewijzigd:

1. In het eerste lid wordt de zinsnede "Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen" vervangen door:
Hij aan wiens schuld te wijten is dat in een geautomatiseerd werk gegevens die door middel van dat werk zijn opgeslagen, worden verwerkt of overgedragen.

2. In het tweede lid wordt de zinsnede "die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk" vervangen door:
die zijn bestemd om schade aan te richten in een geautomatiseerd werk.

Ka

Artikel 371, tweede lid, wordt als volgt gewijzigd:
1. De zinsnede "door een ambtenaar van de telefonie of door andere personen belast met de dienst van een ten algemenen nutte gebezigde telefooninrichting" wordt vervangen door:
door een persoon, werkzaam bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst.

2. De woorden "die instelling" worden vervangen door:
dat netwerk of die dienst.

Kb

Artikel 372 wordt als volgt gewijzigd:
1. Voor de bestaande tekst wordt een 1. geplaatst.
2. Een nieuw lid wordt toegevoegd, dat luidt:

2. Met dezelfde straf wordt gestraft de persoon, werkzaam bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, die opzettelijk en wederrechtelijk een gesloten elektronisch bericht dat ter verdere verzending is opgeslagen in het geautomatiseerd werk van die aanbieder, opent, dit bericht inziet of de inhoud ervan aan een ander bekendmaakt.

L

Artikel 418 komt te luiden:

Artikel 418
1. Hij die als tussenpersoon in de uitoefening van zijn beroep of bedrijf enige uiting in gesproken woord, beeld of geschrift van strafbare aard afkomstig van een ander openbaar maakt of verspreidt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie, indien:
a. de dader noch bekend is, noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de tussenpersoon is bekendgemaakt;
b. de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, heeft nagelaten alle handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding.
2. Onder de tussenpersoon, bedoeld in het eerste lid, wordt verstaan: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift afkomstig van derden, tenzij op deze persoon het bij of krachtens de Mediawet bepaalde van toepassing is.

M

Artikel 419 komt te luiden:

Artikel 419
1. Hij die enig geschrift of enige afbeelding drukt van strafbare aard, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie, indien:
a. de persoon op wiens last het stuk is gedrukt noch bekend is, noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, door de drukker is bekendgemaakt;
b. de drukker op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, heeft nagelaten alle handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van de openbaarmaking of verspreiding.

Artikel II

Het Wetboek van Strafvordering, zoals dit luidt indien het bij koninklijke boodschap van 23 juli 1993 ingediende voorstel van wet tot partiële wijziging van het Wetboek van Strafvordering (herziening van het gerechtelijk vooronderzoek; 23 251) en het bij koninklijke boodschap van 17 juni 1997 ingediende voorstel van wet tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden; 25 403) tot wet zijn verheven en in werking zijn getreden, wordt als volgt gewijzigd:

A

Artikel 125i wordt als volgt gewijzigd:

1. Het eerste lid komt te luiden:

1. Tijdens het gerechtelijk vooronderzoek kan de rechter-commissaris, ambtshalve of op vordering van de officier van justitie, het bevel geven dat hij van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die kunnen dienen om de waarheid aan de dag te brengen en die zijn opgeslagen in een geautomatiseerd werk, deze gegevens zal vastleggen, de rechter-

commissaris tot deze gegevens toegang zal verlenen of deze gegevens zal overbrengen naar de griffie van de rechtbank, een en ander binnen de termijn en op de wijze bij het bevel te bepalen.

2. Het tweede lid, onderdeel 1, komt te luiden:

1°. waarvan redelijkerwijs kan worden vermoed dat die door de verdachte zijn ingevoerd, dat die voor hem zijn bestemd, dat die tot het begaan van het strafbare feit hebben gediend of dat met betrekking tot die gegevens het strafbare feit is gepleegd;

3. Onder vernummering van het derde lid tot vierde lid wordt na het tweede lid een nieuw lid ingevoegd, dat luidt:

3. Op gesloten elektronische berichten die ter verdere verzending zijn opgeslagen in het geautomatiseerd werk van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, kan het bevel slechts betrekking hebben voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem zijn bestemd of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd.

B

In artikel 125j, tweede lid, vervallen de woorden "voor zover".

C

Artikel 125k wordt "bij een doorzoeking of bij toepassing van artikel 125j" vervangen door: bij gelegenheid van een doorzoeking of de toepassing van artikel 125j.

D

Artikel 125m komt te luiden:

Artikel 125m

1. Een bevel als bedoeld in artikel 125i, eerste lid, wordt niet gegeven aan de verdachte. Een bevel als bedoeld in artikel 125k kan slechts aan de verdachte worden gegeven indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid.
2. De personen, bedoeld in artikel 96a, derde lid, kunnen zich verschonen van de nakoming van de in het eerste lid bedoelde bevelen.

E

Onder vernummering van artikel 125n tot artikel 125q worden na artikel 125m drie nieuwe artikelen ingevoegd, die luiden:

Artikel 125n
Bij gelegenheid van een doorzoeking of de toepassing van een van de bevoegdheden, bedoeld in deze Afdeling, is de rechter-commissaris bevoegd te bepalen dat van de inhoud van gesloten elektronische berichten die ter verdere verzending zijn opgeslagen in het geautomatiseerd werk van

een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, zal worden kennis genomen, voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem zijn bestemd of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd.

Artikel 125o
1. Indien bij een onderzoek in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbaar 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 strafbaar feit of ter voorkoming van nieuwe strafbare feiten.
2. Onder ontoegankelijkmaking van gegevens opgeslagen in een geautomatiseerd werk wordt verstaan het treffen van maatregelen ter voorkoming dat de beheerder van dat geautomatiseerd 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 wissen van de gegevens uit het geautomatiseerd 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 geautomatiseerd werk worden gesteld.

Artikel 125p
1. Leidt een doorzoeking of de toepassing van de bevoegdheid tot inbeslagneming of van één van de bevoegdheden, bedoeld in deze Afdeling, tot vastlegging van gegevens opgeslagen door middel van een geautomatiseerd werk of tot ontoegankelijkmaking van gegevens opgeslagen in een geautomatiseerd werk, dan wordt zo spoedig mogelijk aan de beheerder van dat geautomatiseerd werk en, voor zover dat redelijkerwijs mogelijk is, aan andere belanghebbenden een opgave van deze gegevens gedaan.
2. De officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris kan bepalen dat de in het eerste lid bedoelde opgave aan een belanghebbende achterwege blijft indien en zolang dit noodzakelijk is voor de uitoefening van een van de bevoegdheden van titel IVa, V of Va ten aanzien van die persoon.

F

Artikel 125q, eerste lid, komt te luiden:

1. Zodra blijkt dat de gegevens die zijn vastgelegd bij gelegenheid van een doorzoeking of de toepassing van de bevoegdheid tot inbeslagneming of van één van de bevoegdheden, bedoeld in deze Afdeling, van geen betekenis zijn voor het onderzoek, worden zij vernietigd.

G

Artikel 126i wordt als volgt gewijzigd:
1. Het eerste lid komt te luiden:

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 bevelen dat een opsporingsambtenaar:
a. goederen afneemt van de verdachte,

b. gegevens afkomstig uit een geautomatiseerd werk door tussenkomst van een openbaar telecommunicatienetwerk afneemt van de verdachte, of
c. diensten verleent aan de verdachte.

2. In het derde lid, onderdeel c, wordt na "goederen" ingevoegd:
, gegevens.

H

Aan artikel 126m worden vier nieuwe leden toegevoegd, die luiden:

5. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij gelegenheid van de toepassing van het eerste lid tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in het eerste lid bedoelde telecommunicatie, het bevel 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.
6. Het bevel, bedoeld in het vijfde lid, kan slechts aan de verdachte worden gegeven indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid.
7. De personen, bedoeld in artikel 96a, derde lid, kunnen zich verschonen van de nakoming van dit bevel.
8. Op het bevel, bedoeld in het vijfde lid, is artikel 126l, vierde, zesde en zevende lid, van overeenkomstige toepassing.

I

Artikel 126q wordt als volgt gewijzigd:
1. Het eerste lid komt te luiden:

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar:
a. goederen afneemt van een persoon 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,
b. gegevens afkomstig uit een geautomatiseerd werk door tussenkomst van een openbaar telecommunicatienetwerk afneemt van die persoon, of
c. diensten verleent aan die persoon.

2. In het derde lid, onderdeel c, wordt na "goederen" ingevoegd:
, gegevens.

J

Aan artikel 126t worden vier nieuwe leden toegevoegd, die luiden:

5. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij gelegenheid van de toepassing van het eerste lid tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in het eerste lid bedoelde telecommunicatie, het bevel 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.

6. Het bevel, bedoeld in het vijfde lid, kan slechts aan de verdachte worden gegeven indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid.
7. De personen, bedoeld in artikel 96a, derde lid, kunnen zich verschonen van de nakoming van dit bevel.
8. Op het bevel, bedoeld in het vijfde lid, is artikel 126s, vierde, zesde en zevende lid, van overeenkomstige toepassing.

K

Artikel 354 komt te luiden:

Artikel 354

1. In de gevallen, bedoeld in artikel 353, eerste lid, neemt de rechtbank tevens een beslissing over de met toepassing van artikel 125o ontoegankelijk gemaakte gegevens indien de desbetreffende maatregelen nog niet zijn opgeheven.
2. De rechtbank kan gelasten dat de gegevens worden vernietigd indien het gegevens betreft met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan, voor zover de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. In alle andere gevallen gelast zij dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerd werk worden gesteld.

L

Artikel 552a wordt als volgt gewijzigd:
1. Het eerste lid komt te luiden:

1. De belanghebbenden kunnen schriftelijk zich beklagen over inbeslagneming, over het gebruik van inbeslaggenomen voorwerpen, over het uitblijven van een last tot teruggave, over de kennisneming of het gebruik van gegevens opgeslagen door middel van een geautomatiseerd werk en vastgelegd tijdens een huiszoeking, over de kennisneming of het gebruik van gegevens, als bedoeld in de artikelen 100, 101, 114, 125i en 125j, alsmede over de ontoegankelijkmaking van gegevens opgeslagen in een geautomatiseerd werk, bedoeld in artikel 125o, de opheffing van de desbetreffende maatregelen of het uitblijven van een last tot zodanige opheffing.

2. In het tweede lid wordt "na de inbeslagneming der voorwerpen of de kennisneming der gegevens" vervangen door:
na de inbeslagneming van de voorwerpen of de kennisneming of ontoegankelijkmaking van de gegevens.
3. In het derde lid wordt "of kennisneming" telkens vervangen door:
, kennisneming of ontoegankelijkmaking.
4. In het vierde lid, tweede volzin, wordt na "hetzelfde voorwerp" ingevoegd:
of dezelfde gegevens.

M

Na artikel 552f wordt een artikel ingevoegd, dat luidt:

Artikel 552fa

1. Bij een afzonderlijke rechterlijke beschikking op vordering van de officier van justitie kan worden gelast dat de met toepassing van artikel 125o ontoegankelijk gemaakte gegevens worden vernietigd indien het gegevens betreft met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan, voor zover de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten.
2. Aan de beheerder van het geautomatiseerd werk waarin de gegevens zijn of waren opgeslagen wordt een afschrift van de vordering betekend.
3. Artikel 552f, eerste, vierde, vijfde en zesde lid, is van overeenkomstige toepassing.
4. Indien het gerecht de vordering afwijst, gelast het dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerd werk worden gesteld.

Artikel III

1. Artikel 125n van het Wetboek van Strafvordering is niet van toepassing op gesloten elektronische berichten als bedoeld in dat artikel die voorafgaand aan het tijdstip van inwerkingtreding van deze wet zijn vastgelegd bij gelegenheid van een doorzoeking of de toepassing van een van de bevoegdheden, bedoeld in de Zevende Afdeling van Titel IV van het Eerste Boek van het Wetboek van Strafvordering.
2. Artikel 125m, eerste lid, tweede volzin, en de artikelen 126m, vijfde lid, en 126t, vijfde lid, van het Wetboek van Strafvordering zijn niet van toepassing in zaken waarin de betrokken doorzoeking vóór het tijdstip van inwerkingtreding van deze wet heeft plaatsgevonden onderscheidenlijk het betrokken bevel tot het opnemen van telecommunicatie vóór het tijdstip van inwerkingtreding van deze wet is uitgevaardigd.
3. Een bevel aan een opsporingsambtenaar tot het afnemen van een bepaald persoon van gegevens afkomstig uit een geautomatiseerd werk door tussenkomst van een openbaar telecommunicatienetwerk, welk bevel is uitgevaardigd voorafgaand aan het tijdstip van inwerkingtreding van deze wet, geldt als een bevel als bedoeld in de artikelen 126i, eerste lid, onderdeel b, en 126q, eerste lid, onderdeel b, van het Wetboek van Strafvordering, indien het aan de in het toepasselijke artikel gestelde eisen voldoet.

Artikel IV

De artikelen van deze wet treden in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren wie zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Justitie,

MEMORIE VAN TOELICHTING

1. Inleiding: inhoud van dit wetsvoorstel

Het ontstaan en de ontwikkeling van de computer had en heeft ingrijpende gevolgen voor het strafrecht. De Wet computercriminaliteit (Stb. 1993, 33) was het resultaat van een eerste verkenning, naar de toenmalige stand van de techniek, van die gevolgen. In de afgelopen jaren heeft de informatietechnologie zich op stormachtige wijze verder ontwikkeld. In het bijzonder nieuwe technologieën die het mogelijk maken om computers aan elkaar te koppelen en netwerken van computers aan andere netwerken, bieden burgers en overheden ongekende mogelijkheden tot overdracht, verkrijging en bewerking van informatie.

De informatisering van de maatschappij laat de rol van de overheid niet onberoerd. Enerzijds worden de mogelijkheden van de overheid tot controle en sturing, zeker in nationaal verband, kleiner, anderzijds brengt de verantwoordelijkheid van de overheid voor een ordelijk verloop van het verkeer tussen burgers mee dat zij die ordening aanpast aan de gewijzigde omstandigheden opdat ieders gerechtvaardigde belangen zo veel mogelijk juridische bescherming blijven behouden. Dit heeft geleid tot een discussie over de rol van de wetgever op de elektronische snelweg. Een dezer dagen zal ik een rapportage uitbrengen waarin in den brede wordt ingegaan op de uitgangspunten voor wetgeving op de elektronische snelweg (PM).

De Wet computercriminaliteit dient een vervolg te krijgen. Dit wetsvoorstel strekt daartoe. De voorstellen vallen in een aantal onderdelen uiteen, die in het algemeen deel van de toelichting nader zullen worden toegelicht:
A. modernisering van de aansprakelijkheid van tussenpersonen zoals die thans voor uitgevers is neergelegd in artikel 53 van het Wetboek van Strafrecht;
B. invoering van de mogelijkheid om bepaalde computergegevens ontoegankelijk te maken en door de rechter te doen vernietigen;
C. invoering van een verplichting voor aanbieders van telecommunicatie-netwerken of -diensten, alsmede - in bijzondere gevallen - voor de verdachte, om mee te werken aan het ontsleutelen van gegevens;
D. nadere regeling van de mogelijkheden voor justitie om inzage te verkrijgen in in een geautomatiseerd werk opgeslagen elektronische post;
E. uitbreiding van de door het wetsvoorstel bijzondere opsporingsbevoegdheden voorgestelde pseudokoopbevoegdheid tot het afnemen van gegevens van de verdachte door tussenkomst van een openbaar telecommunicatienetwerk.
Daarnaast bevat het wetsvoorstel nog enkele aanpassingen - meest technische wijzigingen of verduidelijkingen - van de bij de eerste Wet computercriminaliteit ingevoerde bepalingen. Deze zullen in het artikelsgewijze deel van de toelichting kort worden toegelicht.

A. AANSPRAKELIJKHEID VAN TUSSENPERSONEN (Art. I, onderdeel A, B, L en M)

2. Achtergrond

Dit wetsvoorstel wijzigt onder andere de regeling van de uitgeversaansprakelijkheid in het Wetboek van Strafrecht. De directe aanleiding voor deze wijziging wordt gevormd door de maatschappelijke onrust die eind 1995 ontstond over berichten dat op het internationale computernetwerk Internet racistische geschriften, kinderporno en andere strafbare informatie op ruime schaal voorhanden zouden zijn. De kenmerken van dit netwerk brengen mee dat dergelijk materiaal snel en op eenvoudige wijze wereldwijd verspreid kan worden en voor een groot publiek beschikbaar kan

worden gemaakt, terwijl de afzenders of verdere verspreiders moeilijk traceerbaar zijn of niet grijpbaar voor nationale overheden omdat ze zich in het buitenland bevinden. De vraag kwam op wat in dit geval de rol is van de zogenaamde Internet Service Providers. Dit zijn bedrijven die tegen betaling toegang verlenen tot Internet, alsmede andere diensten ten aanzien van Internet aanbieden (*e-mail,* het opzetten van *Web-sites,* toegang tot *newsgroups*). Ik heb mij bij verschillende gelegenheden op het standpunt gesteld dat de providers reeds naar huidig recht onder omstandigheden strafrechtelijk aansprakelijk zijn - te denken valt aan medeplichtigheid - voor de via hen verspreide strafbare informatie mits zij op de hoogte waren van de aard van de informatie, althans indien het aan hun ernstige nalatigheid te wijten was dat het betrokken materiaal op Internet voor het publiek beschikbaar was (zie het antwoord d.d. 19 augustus 1996 op kamervragen over strafbare informatie op de computer van de Technische Universiteit Eindhoven, kamerstukken II 1995/96, Aanh. 1582). Wel heb ik bij die gelegenheden aangekondigd te zullen onderzoeken of de providers een speciale bescherming dienen te krijgen, net als thans in de artikelen 53 en 54 van het Wetboek van Strafrecht is voorzien voor uitgevers en drukkers, opdat zorgvuldig handelende providers niet bevreesd behoeven te zijn voor een strafvervolging.

Bij het bedoelde onderzoek is gebleken dat niet volstaan kan worden met een aanvullende bepaling voor de Internet Service Providers, maar dat een ingrijpende herziening van met name artikel 53 Sr gewenst is. Dit artikel, dat is ontstaan in een tijd waarin de drukpers nog het belangrijkste middel voor de publicatie van meningen en andere uitlatingen was, is ernstig verouderd als gevolg van de ontwikkelingen in deze eeuw op het terrein van de informatievoorziening: radio en televisie werden belangrijke media en kabel en satellieten vergemakkelijken het gegevensverkeer aanzienlijk. De laatste jaren zijn de ontwikkelingen onverminderd doorgegaan. Van een hulpmiddel bij de be- en verwerking van gegevens is de computer geworden tot een belangrijk communicatiemiddel. Dit is tevens illustratie van een andere ontwikkeling: de toenemende convergentie van traditioneel gescheiden media (radio, TV, telefoon, computer). Bij de grondwetsherziening van 1983 werd reeds rekening gehouden met deze en nog onvoorziene ontwikkelingen doordat de drukpersvrijheid werd uitgebreid tot de vrijheid om door radio, televisie of *enig ander middel* gedachten of gevoelens te openbaren, zonder voorafgaand toezicht op de inhoud daarvan (art. 7, tweede en derde lid, Grondwet). Art. 53 Sr verdient een dienovereenkomstige uitbreiding.

3. Uitings- en verspreidingsdelicten

Voor het openbaren van gedachten of gevoelens heeft niemand voorafgaand verlof (wegens de inhoud daarvan) nodig "behoudens ieders verantwoordelijkheid volgens de wet" (art. 7 Grondwet). De laatste clausule doelt met name op de (repressieve) aansprakelijkheid volgens de strafwet. Het Wetboek van Strafrecht kent verschillende bepalingen waarin het doen van bepaalde uitingen wordt strafbaar gesteld: klassieke strafbepalingen, zoals belediging van de Koning (art. 111), opruiing (art. 131), smalende godslastering (art. 147) en smaad (art. 261), en bepalingen van meer recente datum, zoals die betreffende discriminatie (art. 137c en 137d). Naast, en nauw verbonden met, deze uitingsdelicten kent het wetboek strafbaarstellingen die betrekking hebben op de verspreiding van geschriften, afbeeldingen of voorwerpen waarin een bepaalde strafbare uiting is vervat, en op gedragingen die op die verspreiding zijn gericht, zoals het in voorraad hebben van die geschriften e.d. (vgl. artt. 113, 132 en 137e, tweede lid, onder 2, Sr). De vraag is of de omschrijving van deze uitings- en verspreidingsdelicten nog bij de tijd is en voldoende rekening houdt met moderne vormen van communicatie en informatievoorziening. Dat is naar ik meen het geval. Zo kan het via computernetwerken transporteren, kopiëren, ter beschikking stellen en oproepen van gegevens gevat worden onder begrippen als "verspreiden", "in voorraad hebben" of "tentoonstellen". Verder vallen onder "geschriften" niet alleen papieren teksten, maar kunnen er ook lp's, cd's en videobanden

onder worden begrepen, zoals blijkt uit de artikelen 113, tweede lid, 132, tweede lid, 147a, tweede lid, en 261, tweede lid, Sr, waar sprake is van het "ten gehore brengen" van de inhoud van een geschrift. Volgens prof. Remmelink valt er iedere mechanische reproductie van gedachten door het woord onder (Het Wetboek van Strafrecht, losbladig commentaar, aant. 5 op art. 113). Zo verstaan omvat "geschrift" ook een door een computer opgeroepen en op het beeldscherm gebracht gegevensbestand. Met andere woorden: de huidige strafbepalingen behoeven nog geen aanpassing aan nieuwe informatietechnieken; ze zijn tot dusver voldoende "techniek-onafhankelijk". Een recent onderzoek in het kader van het Nationaal Programma van Informatietechnologie en Recht leidde tot deze conclusie (Th. de Roos, G. Schuijt en L. Wissink, Smaad, laster, discriminatie en porno op het Internet, Alphen aan den Rijn/Diegem 1996). Zodra die strafbepalingen niet meer blijken aan te sluiten bij de technische ontwikkelingen, zal de wetgever tot aanpassing moeten overgaan.

Bijzonder kenmerk van de uitings- en verspreidingsdelicten is dat het desbetreffende handelen doorgaans alleen strafbaar is indien het openlijk, in het openbaar, althans met het oog op openbaarmaking, geschiedt. Wat in het privéverkeer tussen twee of meer personen plaatsheeft, is in de regel niet strafbaar. Integendeel, de vrijheid van vertrouwelijke communicatie is een apart in rechte te beschermen belang (vgl. het voorstel tot wijziging van art. 13 Grondwet, kamerstukken II 1996/97, 25 443, en de "freedom of correspondence" van art. 8 EVRM). Hoewel bij de huidige ontwikkelingen de grenzen tussen openbaar en privé, openbaar en besloten verschuiven en soms vervagen, is het nodig aan dit onderscheid vast te houden teneinde in voorkomend geval een juiste afweging tussen botsende grondrechten mogelijk te maken. Criterium voor strafbaarstelling dient te zijn of door bepaald handelen de *openbare* orde is geschaad, zij het wellicht op indirecte wijze. Wat nog besloten is en wat openbaar, dient uiteindelijk aan de interpretatie door de rechter te worden overgelaten. "Openbaar" wil volgens de gangbare opvatting zeggen: ten overstaan van het publiek, algemeen toegankelijk, onverschillig of de toegankelijkheid aan enige voorwaarde of betaling van entree is gebonden (Het Wetboek van Strafrecht, a.w., aant. 4 op art. 131). In deze zin is bijvoorbeeld veel van de communicatie op Internet, met zijn miljoenen en eenvoudig tot stand te brengen aansluitingen, zeker openbaar (de meeste *news groups, Web-sites*). Het verzenden van een *e-mail* aan een bepaalde persoon (of aan een bepaalde, welomschreven groep van personen die als besloten kan worden aangemerkt), daarentegen, zal als privé moeten worden aangemerkt, net als het versturen van een "echte" brief. Hetzelfde geldt voor besloten "babbelboxen".

4. De huidige regeling van de uitgeversaansprakelijkheid

Voor uitgevers en drukkers achtte de wetgever van 1881 een afwijking noodzakelijk van de normale regels van strafrechtelijke aansprakelijkheid voor delicten als belediging en opruiing gepleegd door middel van de drukpers.[1] Waar de Grondwet censuur vanwege de staat verbood, moest worden voorkomen dat uitgevers en drukkers zich gedwongen zouden voelen om in plaats van die staat zelf censuur uit te oefenen op hetgeen zij uitgaven c.q. drukten. Dit gevaar van zelfcensuur werd aanwezig geacht omdat uitgevers en drukkers zich in de normale uitoefening van hun beroep schuldig zouden kunnen maken aan medeplichtigheid of medeplegen wanneer zij een geschrift met een strafbare inhoud uitgaven of drukten. Voor dat geval werden de artikelen 53 en 54 in het wetboek opgenomen, die hen van vervolging vrijwaarden mits zij een bepaalde zorgvuldigheid in acht namen: de uitgever of drukker moest op het betrokken stuk zijn naam en woonplaats vermelden en hij moest de dader - in het geval van de drukker: degene op wiens last het stuk is gedrukt -, dat

[1] Zie voor de wetsgeschiedenis van de artikelen 53 en 54 Sr H.J. Smidt, Geschiedenis van het Wetboek van Strafrecht, eerste deel, Haarlem 1881, blz. 422 e.v.

wil zeggen degene van wie het strafbare stuk afkomstig was, bekendmaken (als die nog niet bekend was). Voldeed de uitgever of drukker niet aan deze voorwaarden, dan genoot hij niet de bescherming van de artikelen 53 of 54 en waren op hem de normale regels van strafrechtelijke aansprakelijkheid van toepassing. Hetzelfde gold wanneer de uitgever of drukker in zee ging met iemand die niet "grijpbaar" was voor justitie omdat hij niet vervolgbaar was of buiten het rijk in Europa woonde. In dat geval droeg de uitgever of drukker er aan bij dat de aansprakelijke persoon buiten de handen van justitie bleef en kon hij niet terugvallen op artikel 53 of 54. Bij dit alles dient te worden aangetekend dat de uitgever en drukker - onder de genoemde voorwaarden - alleen van vervolging werden gevrijwaard indien zij zich beperkten tot hun normale arbeid, hetgeen tot uitdrukking werd gebracht door de woorden "wordt de uitgever *als zoodanig* niet vervolgd". Wie geschriften met een strafbare inhoud uitgaf of drukte die hij zelf had geschreven of tot het schrijven waarvan hij een ander had uitgelokt, verdiende geen bijzondere bescherming als uitgever of drukker.

Strijdpunt in de Tweede Kamer was in hoeverre de uitgever of drukker voor de inhoud van het betrokken stuk kon worden gestraft indien de voorwaarden van artikel 53 of 54 niet waren vervuld. Een deel - en met hen minister Modderman - vond dat de uitgever en drukker alleen volgens de normale regels als medeplichtige of medepleger konden worden gestraft. Dit betekende doorgaans dat bewezen moest worden dat zij kennis hadden gehad van de inhoud van het geschrift. Anders zou niet voldaan zijn aan het bestanddeel "opzettelijk" zoals dit voorkomt bij medeplichtigheid en de meeste uitingsdelicten . Volgens een ander deel van de Kamer daarentegen zou dit neerkomen op een vrijbrief voor de uitgever en drukker om alles uit te geven of te drukken, mits zij er geen kennis van namen. Als compromis zijn uiteindelijk de artikelen 418 en 419 ontstaan, die strafbaar stellen het uitgeven c.q. drukken van een geschrift of afbeelding van strafbare aard terwijl niet aan de voorwaarden van artikel 53 of 54 is voldaan (d.w.z. indien de dader noch bekend is noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, is bekendgemaakt, of indien de uitgever of drukker wist of moest verwachten dat de dader (of persoon op wiens last het stuk is gedrukt) op het tijdstip van de uitgave niet vervolgbaar of buiten het Rijk in Europa gevestigd zou zijn). In dat geval is de aansprakelijkheid van de uitgever of drukker, die als een aansprakelijkheid *sui generis* werd beschouwd, gegrond op onvoldoende voorzichtigheid bij het uitgeven of drukken.

Zoals gezegd zijn de artikelen 53 en 54 Sr, anders dan de uitings- en verspreidingsdelicten, niet meer bij de tijd. Ik wijs op de volgende punten.

- De klassieke drukpers is al lang niet meer het enige middel voor de openbaarmaking en verspreiding van uitingen. Radio, TV en computernetwerken zijn erbij gekomen. Tegelijkertijd vervagen de grenzen tussen deze middelen.
- Naast uitgevers en drukkers zijn nieuwe bedrijven ontstaan met een vergelijkbare, intermediaire functie in de informatiemaatschappij. Denk aan omroepen, kabelbedrijven en Internetproviders. En ook hier vervagen de grenzen (vgl. grote uitgevers die *on line* gaan).
- De wetgever van 1881 dacht bij drukpersdelicten aan de primaire openbaarmaking met behulp van de drukpers. Dáárin school het gevaar van (zelf-)censuur en niet in de verdere verspreiding van het gedrukte. Distributeurs zoals boekhandels verdienden dus geen bijzondere bescherming (H.J. Smidt, a.w., tweede deel, blz. 44-48). Deze opvatting is in de huidige informatiemaatschappij niet meer houdbaar: zij doet geen recht aan het grote belang van de verspreiding van informatie en de daartoe beschikbare middelen en miskent dat het onderscheid tussen drukken, uitgeven en verspreiden vervaagt.

5. De voorgestelde regeling

Ik meen dat het wenselijk is de artikelen 53 en 54 Sr op de genoemde punten aan te passen en te moderniseren. Ik noem daarvoor een aantal redenen: ten eerste het grote belang van een onbelemmerde informatievoorziening in een democratische rechtsstaat, voorts de opdracht aan de overheid, uitgedrukt in artikel 7 Grondwet, om de vrijheid van de burger om door enig middel gedachten of gevoelens te openbaren te waarborgen en te bevorderen, en tot slot de steeds belangrijker wordende rol van personen die een intermediaire functie vervullen in de informatiemaatschappij. Zo veel mogelijk dient te worden voorkomen dat deze tussenpersonen zich gedwongen voelen tot een vorm van zelfcensuur. Dit neemt overigens niet weg dat zij een zekere verantwoordelijkheid hebben voor wat zij doorgeven, namelijk voor zover de betrokken informatie voor het publiek toegankelijk wordt gemaakt, en dat derhalve van hen een bepaalde zorgvuldigheid kan worden geëist. Nemen zij die zorgvuldigheid niet in acht, bijvoorbeeld door een anoniem geschrift van strafbare aard te verspreiden waarvan zij de aard kennen of redelijkerwijs kunnen vermoeden, dan moeten zij voor de strafrechter ter verantwoording kunnen worden geroepen. Beide aspecten - bescherming tegen vervolging van de tussenpersoon die normaal zijn beroep uitoefent, en aansprakelijkheid indien niet een zekere zorgvuldigheid in acht wordt genomen - dienen in een moderne regeling van de uitgeversaansprakelijkheid tot uitdrukking te worden gebracht.

De vraag zou kunnen worden gesteld of de bedoelde tussenpersonen - ook de nieuwe tussenpersonen zoals Internetproviders - niet reeds onder het wettelijke begrip "uitgever" kunnen worden begrepen. Daartoe zou een extensieve interpretatie nodig zijn. Hoewel niet ondenkbaar is dat de rechtspraak een dergelijke interpretatie zou willen aanvaarden, ben ik van mening dat uit een oogpunt van rechtszekerheid een nieuwe wettelijke regeling, aangepast aan de moderne tijd, de voorkeur verdient. Ik word hierin gesteund door het reeds aangehaalde onderzoek van De Roos c.s. (Smaad, laster, discriminatie en porno op het Internet, a.w., blz. 200).

In de voorgestelde regeling wordt de uitgever in artikel 53 Sr vervangen door de professionele "tussenpersoon" die door enig middel (drukpers, radio, netwerk) informatie afkomstig van derden beschikbaar maakt voor het publiek. Doel van deze wijziging is deze tussenpersoon *als zodanig* te vrijwaren van vervolging wegens zijn betrokkenheid bij uitings- of verspreidingsdelicten, mits voldaan is aan de in artikel 53 neergelegde voorwaarden. Is niet aan een van die voorwaarden voldaan, dan kan hij volgens de gewone regels die gelden voor daderschap en deelneming, worden gestraft en voorts wegens de overtreding van artikel 418 Sr, dat daartoe ook zal worden aangepast.

De nieuwe regeling van artikel 53 biedt tussenpersonen niet slechts bescherming bij het gebruik van de klassieke drukpers, maar ook bij het gebruik van "enig ander middel voor de openbaarmaking of verspreiding" van informatie ("uitingen in gesproken woord, beeld of geschrift "). Deze omschrijving omvat ook de modernere media, zoals radio en TV en, van recente datum, computernetwerken. De regeling biedt bovendien niet alleen bescherming bij de primaire openbaarmaking maar ook bij de verspreiding. Voor het begrip "tussenpersoon" is gezocht naar een techniekonafhankelijke omschrijving van de *functie* van uitgever in de moderne informatiemaatschappij: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in gesproken woord, beeld of geschrift afkomstig van derden.[2]

Wie genieten volgens het voorstel voortaan de bescherming van artikel 53 Sr? Ik geef een - niet-limitatieve - opsomming van professionele "tussenpersonen": de (klassieke) uitgever, exploitanten van bioscopen, Internet-providers, boekhandels, bibliotheken. Ook de personen die onder de Mediawet vallen (omroepverenigingen, beheerders van draadomroepinrichtingen), zijn onder omstandigheden aan te merken als tussenpersonen, zodat zij op de in artikel 53 genoemde

---

[2] Van Dale omschrijft de uitgever als: "persoon die zich beroepshalve belast met het laten drukken of anderszins vermenigvuldigen van geschriften, om die aan het publiek te verkopen".

voorwaarden gevrijwaard zijn van strafrechtelijke vervolging. Voorgesteld wordt echter om deze personen uit te zonderen van de werking van de strafbaarstelling van artikel 418 Sr, zodat het (bestuursrechtelijke) regime van de Mediawet niet wordt doorkruist. Drukkers vallen niet onder het begrip tussenpersoon, tenzij zij zelf ook de gedrukte werken verspreiden. Artikel 54 dient dan ook voor het eigenlijke drukkerswerk te worden gehandhaafd.

De eerste twee voorwaarden die artikel 53 Sr thans stelt aan uitsluiting van vervolging, zijn in de nieuwe opzet - behoudens enkele tekstuele wijzigingen - gehandhaafd: de tussenpersoon dient bij de openbaarmaking of verspreiding zijn identiteit bekend te maken en hij dient op de eerste aanmaning nadat tot een gerechtelijk vooronderzoek is overgegaan, de naam van de dader (c.q. auteur) bekend te maken. Dit geldt niet voor de derde voorwaarde, betreffende de "grijpbaarheid" van de (hoofd)dader van het uitingsdelict. Deze voorwaarde houdt thans in dat de dader ten tijde van de uitgave binnen Nederland (thans nog "het Rijk in Europa") gevestigd was. Deze voorwaarde stamt uit een tijd dat van grensoverschrijdende strafbare feiten - althans op het onderhavige terrein - weinig sprake was. Zat de dader - bij uitzondering - wel in het buitenland, dan achtte men het gerechtvaardigd terug te "grijpen" op de uitgever. Bij de huidige internationalisering van het (informatie)verkeer, waarbij auteurs en verspreiders vaak in verschillende landen zijn gevestigd, zou handhaving van de op genoemde wijze geformuleerde voorwaarde de reikwijdte van de vervolgingsuitsluitingsgrond voor tussenpersonen echter onaanvaardbaar beperken. Dit geldt met name voor tussenpersonen op een wereldomspannend netwerk als Internet. Zij zouden slechts zelden een beroep op art. 53 hebben. Voorts is het zo dat in toenemende mate via rechtshulp- en uitleveringsverdragen instrumenten ter beschikking komen waardoor geciviliseerde staten in goede samenwerking en op een adequate wijze internationale criminaliteit kunnen aanpakken, zodat van staten mag worden verwacht dat ze deze instrumenten gebruiken - en verder ontwikkelen - om de (hoofd)dader te kunnen vervolgen.

Het is dus zaak de verantwoordelijkheid van tussenpersonen op andere wijze vorm te geven, onafhankelijk van de rechtsmacht en de feitelijke mogelijkheden die Nederland heeft met betrekking tot de vervolging van de auteur. De oplossing die is gekozen, knoopt aan bij de mogelijkheden die de (zich hier te lande bevindende) tussenpersoon heeft om een einde te maken aan de strafbare verspreiding van bepaalde uitingen. Daartoe wordt de derde voorwaarde van artikel 53 aldus geformuleerd dat "de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding." Deze voorwaarde kan, afhankelijk van de omstandigheden en de stand van de techniek, meebrengen dat de tussenpersoon in contact treedt met de klant die via hem strafbare uitingen verspreidt en zo nodig stappen tegen deze onderneemt, of dat de tussenpersoon de technische maatregelen neemt om een einde te maken aan de verspreiding. Wat precies van de tussenpersoon kan worden gevergd, zal van geval tot geval, mede afhankelijk van de stand van de techniek, moeten worden beoordeeld door de officier van justitie die een gerechtelijk vooronderzoek heeft gevorderd en de tussenpersoon heeft gemaand aan de verspreiding een eind te maken; de officier van justitie staat daarbij onder controle van de rechter: in eerste instantie de rechter-commissaris en eventueel, als de officier van justitie toch tot vervolging overgaat, de zittingsrechter.

De voorgestelde derde voorwaarde van art. 53 Sr stelt eisen aan het optreden van de tussenpersoon achteraf, wanneer eenmaal volgens de normale regels van het strafrecht aansprakelijkheid is ontstaan. Dit is ook in de formulering tot uitdrukking gebracht ("op de eerste aanmaning... alle handelingen heeft verricht"). Door adequate maatregelen achteraf kan de tussenpersoon alsnog aan aansprakelijkheid ontkomen. Deze kwestie dient te worden onderscheiden van de vraag wanneer strafrechtelijke aansprakelijkheid van de tussenpersoon *ontstaat* en met name wanneer sprake is van verwijtbaar handelen van de tussenpersoon. In de volgende paragraaf ga ik in op de mate van zorgvuldigheid die van de tussenpersoon wordt geëist, wil hij voorkomen dat iedere aansprakelijkheid ontstaat.

Tot slot zij benadrukt dat artikel 53 de aansprakelijkheid volgens de strafwet niet uitbreidt maar juist beperkt. Met het nieuwe begrip "tussenpersoon" is dan ook geenszins beoogd meer personen onder het bereik van de strafwet te brengen dan tot nu toe het geval is. Integendeel, anders dan voorheen profiteren bijv. ook boekhandelaren en bioscoopexploitanten van de vervolgingsuitsluitingsgrond. Voorts is het zo dat de eisen die gelden voor daderschap en deelneming, onverkort op de tussenpersonen van toepassing zijn. Niet gerechtvaardigd is dan ook de vrees, die hier en daar wel doorklinkt, dat voortaan ook personen of bedrijven strafrechtelijk aansprakelijk zouden kunnen worden gesteld die louter als "doorgeefluik" voor uitingen fungeren en niet over de (technische) mogelijkheden beschikken om aan die uitingen een einde te maken. In zo'n geval zal van daderschap of medeplichtigheid geen sprake zijn. Daarvoor is immers een zekere beschikkingsmacht of macht tot ingrijpen vereist. Ik wijs ook op de criteria van het IJzerdraad-arrest (HR 23 februari 1954, NJ 1954, 378), die gelden voor functioneel daderschap: vermocht betrokkene erover te beschikken en placht hij te aanvaarden dat de litigieuze handelingen plaatsvonden? Zij die slechts de technische middelen verschaffen die noodzakelijk zijn voor de overdracht van of toegang tot bepaalde informatie, zullen in het algemeen dus niet als tussenpersoon aansprakelijk kunnen worden gesteld.

6. De aansprakelijkheid van de tussenpersoon; onvoldoende zorgvuldigheid

De keerzijde van de bescherming van de tussenpersoon op grond van artikel 53 Sr is dat deze persoon onder omstandigheden strafrechtelijk aansprakelijk is voor zijn rol bij een uitings- of verspreidingsdelict dan wel als dader van artikel 418 Sr. Het niet voldoen aan de voorwaarde van art. 53 leidt op zichzelf nog niet tot aansprakelijkheid van de tussenpersoon. Daarvoor geldt de algemene eis dat de tussenpersoon een verwijt kan worden gemaakt van het strafbare feit. Welke mate van verwijtbaarheid aanwezig moet zijn en of die moet worden bewezen, is afhankelijk van de delictsomschrijving. De uitings- en verspreidingsdelicten bevatten bijvoorbeeld vaak het bestanddeel "indien hij weet of ernstige reden heeft te vermoeden" dat het geschrift een opruiende, discriminerende enz. inhoud heeft. In deze gevallen zal de opzet of schuld van de tussenpersoon moeten worden telastegelegd en bewezen. Verder bevat artikel 418 Sr - in de thans voorgestelde tekst - weliswaar geen schuldbestanddeel, maar dit neemt niet weg dat het schuldbeginsel meebrengt dat de tussenpersoon wel enig verwijt moet kunnen worden gemaakt van het feit dat de door hem verspreide informatie een strafbare inhoud heeft. Wist hij niets en behoefde hij ook niets te weten, dan kan hij zich beroepen op de strafuitsluitingsgrond afwezigheid van alle schuld.

De vraag is derhalve welke mate van verwijtbaarheid minimaal vereist is om de tussenpersoon strafrechtelijk aansprakelijk te kunnen stellen voor de inhoud van de door hem verspreide informatie (hetzij via deelneming aan een uitings- of verspreidingsdelict, hetzij via art. 418 Sr); anders gezegd: welke mate van zorgvuldigheid dient de tussenpersoon te betrachten wil hij zich van het gevaar van een strafrechtelijke veroordeling vrijwaren? Dit zijn moeilijke vragen, die tot scherpe debatten aanleiding geven. Gelet op de massaliteit van het tegenwoordige informatieverkeer is het niet verwonderlijk dat vooral verspreiders er beducht voor zijn om verantwoordelijk te worden gehouden voor ieder bericht dat via hen wordt verspreid. Sommige Internetproviders gaan zelfs zover dat zij iedere strafrechtelijke aansprakelijkheid afwijzen, onder het motto "geen boodschap aan de boodschap". Dit standpunt kan echter niet als juist worden aanvaard. De boodschapper is onder omstandigheden aansprakelijk, afhankelijk van de aard van de door hem verrichte dienst in verband met de reikwijdte van de betrokken strafbaarstelling. Zo valt de communicatie in besloten kring, dat wil zeggen tussen twee of enkele privépersonen, in de regel niet onder het bereik van de uitings- en verspreidingsdelicten; deze communicatie is zelfs beschermd (zie o.a. artt. 13 Grondwet, 8 EVRM, 139c Sr). A fortiori zijn degenen die die communicatie technisch mogelijk maken, niet aansprakelijk voor de inhoud van de communicatie. Dit geldt

bijvoorbeeld voor Internetproviders voor zover zij het elektronisch postverkeer (*e-mail*) faciliteren. Anders ligt het wanneer zij een schakel zijn in de openbaarmaking en verspreiding van informatie. Dergelijke openbaarmaking en verspreiding valt doorgaans wel onder de wettelijke omschrijving van uitings- en verspreidingsdelicten, zodat aansprakelijkheid van de tussenpersonen niet a priori kan worden uitgesloten.

Wanneer kan nu worden gezegd dat tussenpersonen zoals Internetproviders onvoldoende zorgvuldigheid hebben betracht en dat de openbaarmaking of verspreiding van strafbare informatie, die door middel van hen heeft plaatsgehad, hun kan worden verweten? Allereerst is dit het geval indien zij op de hoogte waren van de strafbare aard van de informatie en desalniettemin de doorgifte van die informatie niet hebben tegengehouden of stopgezet. Bij uitgevers in de klassieke zin zal wetenschap van de inhoud van het betrokken geschrift aanwezig zijn op het moment van de publicatie, bij verspreiders als de Internetproviders, die dagelijks miljoenen berichten doorgeven, doorgaans niet. Deze laatsten kunnen echter op de hoogte komen bijvoorbeeld doordat ze door een abonnee worden gewezen op een bepaald (bijv. discriminatoir) geschrift dat zich op de computer van de provider bevindt, of via een meldpunt waar meldingen kunnen worden gedaan van de aanwezigheid op het Internet van mogelijk strafbaar materiaal. Neemt de tussenpersoon na een klacht niet tijdig maatregelen teneinde te voorkomen dat het betrokken materiaal verder wordt verspreid, dan kan hij geacht worden dat materiaal (opzettelijk) te hebben openbaargemaakt of verspreid (handelen door nalaten). Ook wanneer de tussenpersoon het strafbare materiaal niet met eigen ogen heeft aanschouwd, maar zich wel bewust was van de aanmerkelijke kans dat strafbare informatie door zijn tussenkomst werd verspreid, kan (voorwaardelijk) opzet worden aangenomen. Stilzitten en de andere kant opkijken, ondanks sterke aanwijzingen voor de aanwezigheid van strafbaar materiaal, vrijwaart de tussenpersoon niet van aansprakelijkheid. Afhankelijk van de delictsomschrijving kan soms ook aanmerkelijke onvoorzichtigheid of grote onoplettendheid (culpa) voldoende grond voor aansprakelijkheid opleveren (vgl. art. 137e lid 1 Sr "naar hij redelijkerwijs moet vermoeden").

Stelselmatig, *preventief* onderzoek, zonder aanwijzingen voor de aanwezigheid van strafbaar materiaal, kan niet van de tussenpersoon worden geëist, nog daargelaten dat het bij de massaliteit van het tegenwoordige informatieverkeer volstrekt onrealistisch is om van tussenpersonen, zoals Internetproviders, te eisen dat ze zich van ieder bericht op de hoogte stellen. Niettemin sluit ik niet uit dat onder omstandigheden een zekere preventieve onderzoeksplicht moet worden aangenomen. Bijvoorbeeld wanneer in een bepaalde newsgroup herhaaldelijk "ongelukken" gebeuren of wanneer de provider weet dat uit een bepaalde hoek regelmatig materiaal van twijfelachtige aard komt, lijkt een steekproefsgewijze controle gerechtvaardigd. Het is uiteindelijk aan de rechter om te beoordelen wanneer het achterwege laten van een dergelijk preventief onderzoek verwijtbaarheid oplevert in zodanige mate dat betrokkene strafrechtelijke aansprakelijk kan worden gehouden.

B. VERNIETIGING VAN COMPUTERGEGEVENS (Art. II, onderdeel E (art. 125o Sv), K, L en M)

7. "Inbeslagneming" van computergegevens

Door de ontwikkeling van computers en informatietechnologie is de band tussen informatie en de informatie*dragers* veel losser geworden. De nieuwe technologie maakt het mogelijk enorme hoeveelheden gegevens op te slaan zonder noemenswaardig ruimtebeslag (een enkele diskette of een harde schijf), razendsnel te verwerken en zo nodig te transporteren naar andere geautomatiseerde werken, die aan het andere eind van de wereld staan. Om deze computergegevens te kunnen lezen heeft men behalve uiteraard computers speciale programmatuur nodig en soms zelfs onstoffelijke "sleutels", wanneer de informatie is beveiligd. Een en ander heeft uiteraard gevolgen voor een

informatiegevoelige sector als de opsporing. De klassieke opsporingsbevoegdheden, zoals inbeslagneming en huiszoeking, zijn in een geautomatiseerde omgeving niet steeds zonder meer toepasbaar. Deze omgeving stelt nieuwe eisen, die o.a. zijn neergelegd in Aanbeveling nr. R (95) 13 van de Raad van Europa "concerning problems of criminal procedural law connected with information technology (aangenomen door het Comité van Ministers op 11 september 1995). Beginsel nr. 2 van het hoofdstuk over "search and seizure" luidt:

> "Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein."

Aanbevolen wordt dus om analoog aan de traditionele zoek- en inbeslagnemingsbevoegdheden bevoegdheden te creëren die het mogelijk maken om onder gelijke voorwaarden computersystemen te doorzoeken en gegevens "in beslag" te nemen. Daarbij dient de rechtsbescherming van belanghebbenden voldoende te zijn gewaarborgd, hetgeen o.a. betekent dat geheime zoekacties naar opgeslagen informatie, zonder dat betrokkene zelfs maar op de hoogte is van het onderzoek tegen hem, niet geoorloofd zijn.

De Aanbeveling van de Raad van Europa maakt onderscheid tussen maatregelen met het oog op de waarheidsvinding en maatregelen om iets (i.c. gegevens) aan de macht van de betrokkene te onttrekken teneinde te voorkomen dat deze er (verder) misbruik van maakt of het verspreidt (zie § 54 e.v. van het Explanatory memorandum), een onderscheid dat ook naar Nederlands recht relevant is (vgl. de verschillende doeleinden van inbeslagneming, art. 94, eerste en tweede lid, Sv). De eerste Wet computercriminaliteit (Stb. 1993, 33) richtte zich met name op het eerste, de waarheidsvinding. Zo kunnen het bevel tot toegangverlening tot of overbrenging van gegevens (art. 125i Sv) en de netwerkzoeking (art. 125j Sv) slechts betrekking hebben op gegevens die kunnen dienen om de waarheid aan de dag te brengen. Het gaat er hierbij om van bepaalde gegevens kennis te kunnen nemen; doel is níet om de gegevens aan de beschikkingsmacht van de betrokkene te onttrekken. Doorgaans zal dus volstaan kunnen worden met het maken van een kopie van de betrokken gegevens. Het opeisen van de originele gegevens of het wegnemen van gegevens zonder achterlating van een kopie is in strijd met de, bij iedere opsporingsbevoegdheid in acht te nemen, eisen van proportionaliteit en subsidiariteit. Zodra de bij onderzoek in geautomatiseerde werken vastgelegde gegevens van geen betekenis meer zijn voor het onderzoek, dienen ze - dat wil zeggen alleen de kopieën ten behoeve van justitie - te worden vernietigd (art. 125n Sv).

Het Wetboek van Strafvordering voorziet dus niet in de situatie dat bij een onderzoek in een geautomatiseerd werk gegevens worden aangetroffen die voorwerp uitmaken van een strafbaar feit (bijv. discriminerende uitlatingen (art. 137c Sr) en bedrijfsgeheimen (art. 273)) of met behulp waarvan een strafbaar feit is gepleegd (een computervirus, zie art. 350a Sr). De Nederlandse justitie kan naar huidig recht weinig tegen deze gegevens uitrichten. Waar het gaat om stoffelijke voorwerpen (boeken met een strafbare inhoud, schadelijke werktuigen) beschikken de strafrechtelijke organen over de bevoegdheid tot inbeslagneming en over de sancties van verbeurdverklaring en onttrekking aan het verkeer. Waar het echter gaat om computergegevens waarmee strafbare feiten zijn gepleegd, kan de politie alleen een kopie maken met het oog op de waarheidsvinding. De toepassing van de inbeslagnemingsbevoegdheid ten aanzien van die gegevens - zodanig dat ze uit de macht van de betrokkene worden gehaald - is niet mogelijk aangezien in de visie van de wetgever gegevens geen “goed” zijn (dit is recentelijk bevestigd door de Hoge Raad, zie HR 3 december 1996, NJ 1997, 574 m.nt. ‘tH). Inbeslagneming van de computer met het oog op onttrekking aan het verkeer is evenmin geoorloofd, omdat een computer op zichzelf geen verkeersgevaarlijk voorwerp is en bovendien inbeslagneming uitsluitend vanwege een in de computer aanwezig bestand als disproportioneel moet worden aangemerkt. Alleen wanneer het

strafbare bestand zou zijn vastgelegd op een losse diskette, zou inbeslagneming van die diskette met het oog op onttrekking aan het verkeer wellicht verdedigbaar zijn.

Dit wetsvoorstel voorziet in de hier geschetste lacune en opent de mogelijkheid om computergegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is gepleegd, bij wijze van voorlopige maatregel ontoegankelijk te maken en bij de einduitspraak over het feit of bij afzonderlijke beschikking door de rechter te doen vernietigen. Dit voorstel is in overeenstemming met de Aanbeveling van de Raad van Europa. In de voorgestelde regeling is een aantal elementen overgenomen uit de regeling van de inbeslagneming van voorwerpen met het oog op onttrekking aan het verkeer. Gelet op de analogie ligt dit voor de hand. Wel konden de beoogde maatregelen op een aantal punten eenvoudiger worden geformuleerd. Voorts heb ik er vanaf gezien een aparte strafrechtelijke maatregel, à la de onttrekking aan het verkeer, ten aanzien van gegevens te introduceren. Gelet op het onstoffelijke karakter van gegevens en op het feit dat vermogenswaarde ervan vaak ontbreekt of moeilijk te kwantificeren is, heeft een zelfstandige sanctie t.a.v. gegevens weinig waarde.

8. Ontoegankelijkmaking en vernietiging van gegevens

Allereerst wordt een nieuw artikel 125o Sv voorgesteld, inhoudende een bevoegdheid van de officier van justitie en de rechter-commissaris om te bepalen dat computergegevens met betrekking tot welk of met behulp waarvan het strafbaar feit is gepleegd, *ontoegankelijk worden gemaakt*. De maatregel is slechts mogelijk voor zover zij noodzakelijk is ter beëindiging van het strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Onder "ontoegankelijkmaking van gegevens" wordt verstaan het treffen van maatregelen ter voorkoming dat de beheerder van dat geautomatiseerd 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 wissen van de betrokken bestanden, met behoud van een kopie voor justitie. Dit is de meest voor de hand liggende maatregel. De definitie van ontoegankelijkmaking laat daarnaast echter allerlei andere maatregelen toe, mits die kunnen strekken ter voorkoming van de verdere kennisneming enz. van die gegevens. Een voorbeeld van zulke andere maatregelen is het met behulp van zogenaamde encryptietechnieken als het ware een "slot" zetten op de betrokken bestanden, zodat de beheerder en andere gebruikers van de computer er geen toegang meer toe hebben. Daarnaast is bijvoorbeeld denkbaar dat de toegangspoort van de betrokken computer (tijdelijk) onbruikbaar wordt gemaakt. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is, waarbij uiteraard de eisen van proportionaliteit en subsidiariteit in acht moeten worden genomen.

Uiteraard zal de opsporingsambtenaar trachten alle kopieën en back-ups van de gegevens te achterhalen. De maatregel van ontoegankelijkmaking zou anders zijn effect missen. Dat het niet altijd zal lukken om alle gegevens te achterhalen en ontoegankelijk te maken, doet niet af aan de noodzaak van een daartoe strekkende bevoegdheid. Een effectieve toepassing van de bevoegdheid betekent bijvoorbeeld ook dat bij het wissen van het bestand op een gegevensdrager de technische voorzorgsmaatregelen moeten worden genomen om te voorkomen dat gewiste bestanden achteraf alsnog weer leesbaar worden gemaakt. Van het politie-apparaat mag worden verwacht dat het zich wat dit betreft op de hoogte houdt van de informatietechnologische ontwikkelingen en mogelijkheden en dienovereenkomstig de nodige maatregelen treft die nodig zijn om het gewenste resultaat - de beëindiging van een strafbare situatie en de voorkoming dat verder strafbaar zal worden gehandeld - te bereiken. Soms zal een externe deskundige moeten worden ingeschakeld. In bepaalde gevallen zal de politie haar huidige werkmethoden mogelijk enigszins moeten aanpassen. Zo gaat de politie er nu veelal toe over om van de volledige harde schijf van een geautomatiseerd systeem een kopie te maken teneinde die op het bureau te kunnen onderzoeken op voor de opsporing relevante gegevens. Dit kan in bepaalde situaties, waarin de ongestoorde voortgang van

de bedrijfsvoering in het geding is, een legitieme en evenredige methode van onderzoek zijn (zolang deze gegevens niet ook voor andere doeleinden worden gebruikt). Zij doet echter afbreuk aan de effectiviteit van de voorgestelde maatregel van ontoegankelijkmaking van bepaalde gegevens, aangezien zij de verdachte de tijd geeft om bepaalde bestanden van zijn harde schijf te verwijderen (en naar een onbekende plaats elders over te brengen). In zo'n situatie zal de politie dus ter plaatse moeten trachten strafbare bestanden e.d. te achterhalen en - met toestemming van de officier van justitie of de rechter-commissaris - daartegen de noodzakelijke maatregelen moeten treffen. Ik realiseer me dat dit met name in "netwerkomgevingen" niet altijd een eenvoudige opgave zal zijn

De bevoegdheid tot ontoegankelijkmaking is voorbehouden aan de officier van justitie dan wel, tijdens een gerechtelijk vooronderzoek, de rechter-commissaris. Dit sluit aan bij de bevoegdheidstoedeling in de huidige Zevende Afdeling van Titel IV van Boek 1 en waarborgt dat wanneer bij een onderzoek in een computer door een opsporingsambtenaar (in zijn ogen) dubieuze gegevens worden aangetroffen, deze gegevens niet rauwelings ontoegankelijk kunnen worden gemaakt. Daarvoor is een afstandelijk oordeel, van een officier van justitie of een rechter-commissaris, vereist.

Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen waarmee de gegevens ontoegankelijk zijn gemaakt, dienen de officier van justitie dan wel de rechter-commissaris een daartoe strekkende opdracht te geven. Wordt de ontoegankelijkmaking van de gegevens ongedaan gemaakt, dan herleeft de beschikkingsmacht van degene in wiens computer de gegevens waren aangetroffen. Dit kan op een lijn worden gesteld met de teruggave van een inbeslaggenomen voorwerp aan de beslagene. Opdat deze teruggave ook kan worden geëffectueerd ingeval de betrokken bestanden in de computer van de betrokkene door de politie zijn gewist, dient gelijktijdig met de maatregelen strekkende tot ontoegankelijkmaking van strafbare gegevens ook steeds een kopie van de betrokken gegevens te worden gemaakt. Deze kopie kan dan worden teruggegeven. Teruggave (d.w.z. opheffing van de ontoegankelijkmaking) zal overigens ook moeten geschieden indien de rechter later in de hoofdzaak mocht besluiten om de betrokken gegevens toch niet te laten vernietigen, bijvoorbeeld omdat hij ze niet strafbaar acht, of indien de rechter daartoe beslist op het beklag van een belanghebbende op grond van artikel 552a Sv (zie verderop).

De ontoegankelijkmaking is een voorlopige maatregel. In het nieuwe artikel 354 Sv wordt voorgeschreven dat de rechter bij een materiële einduitspraak over het feit (d.w.z. een veroordeling, een vrijspraak of een ontslag van rechtsvervolging) een definitieve beslissing neemt over de ontoegankelijk gemaakte gegevens, voor zover deze maatregel nog niet door de officier van justitie of de rechter-commissaris is opgeheven. Als hij vaststelt dat de voorwaarden daarvoor aanwezig zijn, kan hij gelasten dat de betrokken computergegevens worden vernietigd. De voorwaarden zijn dezelfde als voor de ontoegankelijkmaking, d.w.z. dat het moet gaan om gegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan en dat de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. In alle andere gevallen gelast de rechter de opheffing van de ontoegankelijkmaking. Niet voorzien is in de mogelijkheid voor de officier van justitie om in het kader van een transactie als voorwaarde te stellen dat de verdachte afstand doet van computergegevens die vatbaar zijn voor vernietiging op last van de rechter (vgl. t.a.v. voorwerpen art. 74, tweede lid, onder b, Sr). Vanwege het ingrijpende karakter van de voorgestelde bevoegdheid, waarmee inbreuk kan worden gemaakt op de vrijheid van meningsuiting, dient zij aan de onafhankelijke rechter te worden voorbehouden. Tussentijds kunnen belanghebbenden zich met een klacht over de ontoegankelijkmaking wenden tot de raadkamer. Hiertoe wordt de beklagmogelijkheid van artikel 552a Sv uitgebreid. Dit is in overeenstemming met Aanbeveling R (95) 13 van de Raad van Europa, die voorschrijft dat de rechtsmiddelen die bestaan ten aanzien van onderzoek ter inbeslagneming van voorwerpen, van overeenkomstige toepassing zijn ten aanzien van het onderzoek in computers.

De rechterlijke last tot vernietiging zal doorgaans meebrengen dat alle bij justitie berustende kopieën worden vernietigd. Indien de gegevens ook nog aanwezig zijn in de computer van de betrokkene - zij het door justitie ontoegankelijk gemaakt door middel van encryptietechnieken -, zullen ook deze moeten worden vernietigd.

9. De voorwaarden voor ontoegankelijkmaking en vernietiging

De ontoegankelijkmaking en uiteindelijke vernietiging van computergegevens dient een tweeledig doel: beîndiging van het strafbaar feit en voorkoming dat met de betrokken gegevens nieuwe strafbare feiten worden gepleegd. Het tweede (preventie) ligt in het verlengde van het eerste (reparatie). Waar sprake is van een voortdurende strafbare toestand vallen beide in feite samen: de ontoegankelijkmaking van de betrokken gegevens maakt een eind aan het strafbaar feit en voorkomt tevens voortzetting daarvan. Waar daarentegen sprake is van een strafbaar feit van voorbijgaande aard (openbaarmaking van strafbare uitlatingen, bekendmaking van bedrijfsgeheimen), valt niets meer te repareren en treedt het preventieve oogmerk van de ontoegankelijkmaking van gegevens op de voorgrond, zij het dat wel is vereist dat met die gegevens een strafbaar feit is gepleegd. Dit betekent dat indien bijvoorbeeld in een *e-mail-box* racistische uitingen worden aangetroffen, dit op zichzelf nog geen grond is om de betrokken gegevens ontoegankelijk te maken en eventueel door de strafrechter te laten vernietigen. Er is immers nog geen reden om aan te nemen dat er iets strafbaars met die gegevens is gebeurd: elektronische post is een vorm van privé-verkeer die niet bestreken wordt door de artikelen 137c Sr e.v. Pas als er wel een redelijk vermoeden is dat met die gegevens op strafbare wijze is gehandeld (bijv. door ze uit te printen en vervolgens te verspreiden), is er (voldoende) grond om ze ontoegankelijk te maken teneinde ze eventueel door de rechter te doen vernietigen.

Er zijn twee categorieën gegevens die zich lenen voor ontoegankelijkmaking c.q. vernietiging in de hier bedoelde zin: gegevens met betrekking tot welke en gegevens met behulp waarvan het strafbaar feit is begaan. Bij de eerste categorie gaat het om gegevens die "voorwerp" zijn van een strafbaar feit, om gegevens die de kern uitmaken van het feit. Hierbij moet allereerst worden gedacht aan gegevens van strafbare aard, d.w.z. gegevens die wegens hun aard niet mogen worden openbaar gemaakt, verspreid enz. Het gaat hier met andere woorden om de strafbare uitingen waarop ook de hiervoor beschreven regeling van de aansprakelijkheid van tussenpersonen betrekking heeft. Daarnaast behoren tot deze categorie de gegevens die weliswaar op zichzelf volstrekt geoorloofd zijn, maar ten aanzien waarvan bepaalde handelingen strafbaar zijn gesteld, zoals schending van auteursrecht of bedrijfsgeheimen of oplichting met het oog op de verkrijging van "gegevens met geldswaarde in het handelsverkeer", bijvoorbeeld klantenbestanden van een gerenommeerd bedrijf (art. 326 Sr). De tweede categorie - gegevens met behulp waarvan een strafbaar feit is begaan - betreft criminele werktuigen bestaande uit gegevensbestanden of computerprogramma's. Voorbeelden hiervan zijn boekhoudprogramma's die standaard een bepaald percentage van een transactie buiten de administratie houden, en virusprogramma's. Het is gewenst dat wanneer politie en justitie bij een onderzoek in een geautomatiseerd werk op dergelijke gegevens stuiten, zij daartegen kunnen optreden, net als het geval is bij inbrekerswerktuigen.

Een apart soort gegevens die onder omstandigheden ontoegankelijk mogen worden gemaakt, wordt gevormd door "gestolen" gegevens. Denk hierbij aan gegevens verkregen als gevolg van "hacking" of aan een gewone diefstal van diskettes met daarop bepaalde waardevolle of anderszins gevoelige informatie. Het eerste geval levert zonder twijfel een strafbaar feit op "met betrekking tot" gegevens in een geautomatiseerd werk, namelijk computervredebreuk (art. 138a lid 2 Sr). In het tweede geval is weliswaar de toeëigening van de op de diskettes vastgelegde informatie op zichzelf niet strafbaar, maar is er een dusdanig verband tussen de diefstal van de (stoffelijke) diskettes en de toeëigening van de informatie, dat mijns inziens gesproken kan worden van

gegevens met betrekking tot welke een strafbaar feit is gepleegd. Voor de vraag of die gegevens vervolgens bij ontdekking door justitie ontoegankelijk mogen worden gemaakt, dient een onderscheid te worden gemaakt. Indien de bekendmaking of het bezit van die gegevens strafbaar is, luidt het antwoord bevestigend (vgl. de diefstal uit een ministerie van dossiers waarin zich staatsgeheimen blijken te bevinden, art. 98 Sr): de ontoegankelijkmaking is dan noodzakelijk ter beëindiging van een strafbaar feit of ter voorkoming van een strafbaar feit. Indien de bekendmaking of het bezit van de betrokken gegevens op zichzelf niet strafbaar is (denk aan vertrouwelijke overheidsinformatie niet zijnde staatsgeheimen, zoals ambtelijke nota's, politieprocessen-verbaal e.d.), is ontoegankelijkmaking alleen geoorloofd als de gegevens kunnen dienen tot het begaan van een strafbaar feit en er bovendien een redelijke kans is dat ze daarvoor ook gebruikt zullen worden. In dat geval is de ontoegankelijkmaking noodzakelijk ter voorkoming van nieuwe strafbare feiten. Een lijst met gestolen passwords zal in het algemeen dus ontoegankelijk mogen worden gemaakt - daarmee kan immers computervredebreuk worden gepleegd -, een politiedossier met gegevens over bepaalde personen (verdenkingen tegen publieke personen, de woonplaats van opsporingsambtenaren) níet, tenzij redelijkerwijs verwacht mag worden dat daarmee een strafbaar feit zal worden gepleegd (afpersing, bedreiging).

In aansluiting hierop wijs ik erop dat de bevoegdheid tot ontoegankelijkmaking geen verplichting inhoudt, maar een discretionaire bevoegdheid waarvan de uitoefening aan de eisen van proportionaliteit en subsidiariteit dient te voldoen. Ingeval bijvoorbeeld bestanden met (ontvreemde) staatsgeheimen worden aangetroffen bij een krantenuitgeverij, zal ontoegankelijkmaking onder omstandigheden niet meer geoorloofd zijn, indien de gegevens reeds ruim bekend zijn gemaakt en de maatregel in een democratische samenleving niet (meer) noodzakelijk kan worden geacht voor het bereiken van het beoogde doel. Vgl. het arrest van het Europese Hof voor de rechten van de mens in de zaak van het Weekblad Bluf! (EHRM 9 februari 1995, Series A, no. 306-A, NJCM-Bulletin 20-4 (1995), p. 480 e.v.).

Voor alle duidelijkheid wijs ik er tot slot op dat alleen gegevens ontoegankelijk kunnen worden gemaakt c.q. vernietigd die in een geautomatiseerd werk zijn opgeslagen. Uitbreiding van de voorgestelde bevoegdheden tot "gegevens" in het algemeen - waaronder bijvoorbeeld ook het gesproken woord of een op papier gestelde tekst valt (zie art. 80quinquies Sr) - acht ik nodig noch gewenst. Ten aanzien van het gesproken woord zijn de voorgestelde maatregelen niet denkbaar, terwijl aan die maatregelen ten aanzien van het geschreven woord geen behoefte bestaat gelet op de reeds bestaande mogelijkheid racistische boeken en tijdschriften e.d. in beslag te nemen en aan het verkeer te onttrekken. In deze laatste gevallen is er immers niet een zo groot verschil tussen de gegevens en de gegevensdragers dat het noodzakelijk is een parte bevoegdheid te creëren ten aanzien van gegevens.

C. ONTSLEUTELING VAN GEGEVENS (Art. II, onderdeel D, H en J)

10. Medewerkingsverplichting t.a.v. versleutelde telecommunicatie

Met de Wet computercriminaliteit is in artikel 125k, tweede lid, van het Wetboek van Strafvordering de bevoegdheid opgenomen om personen die kennis dragen van de versleuteling van gegevens, te verplichten medewerking te verlenen aan de waarheidsvinding door deze kennis ter beschikking te stellen van justitie. Deze bevoegdheid heeft betrekking op onderzoek, ter gelegenheid van een huiszoeking, naar gegevens die zijn *opgeslagen* in een geautomatiseerd werk. Artikel 125k ziet niet op het onderzoek naar *stromende* gegevens, de telecommunicatie. Dat is o.a. geregeld in het huidige artikel 125g betreffende de tapbevoegdheid (volgens het wetsvoorstel bijzondere opsporingsbevoegdheden (25 403) art. 126m en 126t). Anders dan bij de huiszoeking bestaat ten aanzien van het aftappen van telecommunicatie nog geen mogelijkheid voor justitie om

de medewerking van derden, zoals de beheerders van telecommunicatienetwerken, af te dwingen bij het ontsleutelen van gegevensverkeer. Dit wetsvoorstel voorziet hierin op analoge wijze als artikel 125k. Conform het stelsel voorgesteld door wetsvoorstel 25 403 is de officier van justitie degene die de tap beveelt en kan opdragen mee te werken aan het ontsleutelen van gegevens. In beide gevallen heeft hij de (schriftelijke) machtiging van de rechter-commissaris nodig.

Het voorstel illustreert hoe de informatietechnologische ontwikkelingen leiden tot een convergentie van de verschillende vormen van omgang met gegevens: opslag versus transport van gegevens, en de verschillend geregelde opsporingsbevoegdheden ten aanzien van beide vormen. Praktisch gezien worden de verschillen minder groot. Niettemin meen ik dat het wenselijk is te blijven onderscheiden tussen opgeslagen en stromende gegevens. Behalve vanwege de ingevolge het legaliteitsbeginsel vereiste heldere en precieze formulering van strafvorderlijke bevoegdheden is dit ook nodig vanwege een belangrijk verschil in (rechts)gevolg: bij het onderzoek naar opgeslagen gegevens moeten de belanghebbenden zo spoedig mogelijk worden geïnformeerd, zodat zij zich tot de rechter kunnen wenden bij vermeend onrechtmatig politie-optreden, terwijl bij onderzoek naar stromende informatie de uitoefening van de betrokken opsporingsbevoegdheid onontkoombaar enige tijd jegens de belanghebbende geheim moet worden gehouden om als middel effectief te zijn. Dit onderscheid neemt niet weg dat waar mogelijk en nodig de respectievelijke bevoegdheden dienen te worden geharmoniseerd. Het onderhavige voorstel is daarvan een voorbeeld.

De verplichting tot medewerking strekt zich uit tot het ter beschikking stellen van de beschikbare kennis of het aanwenden van bestaande technieken. De verplichting reikt niet zover dat van degene wiens medewerking wordt verlangd, kan worden gevergd dat hij zelf onderzoek doet of instrumenten ontwikkelt. Evenmin vergt de bepaling dat de betrokkene technische voorzieningen aanwezig heeft om aan het bevel te kunnen voldoen. Kan niet worden ontsluierd, dan kan niet via een bevel als thans is voorgesteld, worden geëist dat daartoe alsnog de voorzieningen worden geïnstalleerd. De kosten die moeten worden gemaakt voor de medewerking ad hoc, indien deze medewerking mogelijk is, worden vergoed ingevolge de Wet tarieven in strafzaken.

De sleutel tot het ontcijferen van informatie kan voor de houder ervan van grote waarde zijn. Hij kan er belang bij hebben de kennis daaromtrent niet verder te verspreiden dan strikt nodig is. De bepaling voorziet daarom in de mogelijkheid dat de houder, naar zijn keuze, niet de sleutel ter beschikking stelt, doch deze zelf hanteert om het versleutelde signaal te ontcijferen. Overigens kan dit signaal, voordat het aan de houder werd "aangeboden", op zichzelf ook weer versleuteld zijn met een andere sleutel. Nadere opsporing kan nodig zijn om aldus een keten van versleutelingen ongedaan te maken. De medewerkingsplicht strekt zich niet uit tot dergelijke, voorgaande versleutelingen. Van de houder kan slechts worden verlangd dat hij het signaal in de vorm waarin dit aan hem is aangeboden, ontsleutelt, voor zover hij (nog) over de sleutel beschikt. Zolang er nog geen vordering tot ontsleutelen tot hem is gericht, rust op hem geen verplichting sleutels te bewaren. Dit is anders ten aanzien van aanbieders van telecommunicatienetwerken en -diensten. Voor hen geldt onder het voorstel voor een nieuwe Telecommunicatiewet (25 533) dat hun voorzieningen aftapbaar dienen te zijn (art. 13.1). Deze eis omvat mede de plicht eventueel gebruikte sleutels te bewaren. Zij mogen dus krachtens deze wet geen onontsluierbare cryptografie aan het publiek aanbieden

11. Medewerkingsverplichting voor de verdachte

In het Wetboek van Strafvordering heeft de wetgever tot nu toe als regel aangehouden dat de verdachte niet wordt verplicht actief mee te werken aan het opsporingsonderzoek. Zo kan een bevel tot uitlevering van voor inbeslagneming vatbare voorwerpen niet aan de verdachte worden gegeven (art. 107 lid 1, volgens het wetsvoorstel herziening van het gerechtelijk vooronderzoek (23 251) art. 96a lid 2), kan hij in het kader van een strafrechtelijk financieel onderzoek niet worden verplicht

inzage in bescheiden te geven (art. 126a, tweede lid; de verdachte heet hier "degene tegen wie het onderzoek is gericht") en geldt voor hem geen getuigplicht (art. 29 lid 1). Buiten het Wetboek, in bijzondere wetten, heeft de wetgever echter regelmatig uitzonderingen op deze regel gemaakt en men neemt dan ook aan dat in het Nederlandse strafrecht geen onvoorwaardelijk recht of beginsel geldt dat de verdachte op generlei wijze kan worden verplicht mee te werken aan de bewijsgaring jegens hemzelf. Overigens bestaat ook binnen het Wetboek van Strafvordering reeds een belangrijke uitzondering op de geformuleerde regel, namelijk waar de verdachte verplicht kan worden - eventueel onder fysieke dwang - bloed af te geven ten behoeve van een DNA-onderzoek, zij het dat hier van een verplichting tot *actieve* medewerking geen sprake is (art. 195d lid 1 jo. lid 6).

In dit wetsvoorstel stel ik voor nog een uitzondering te maken op het uitgangspunt van het Wetboek van Strafvordering dat de verdachte niet verplicht kan worden actief mee te werken aan zijn eigen veroordeling. Het betreft de medewerking aan de ontsleuteling van opgeslagen of stromende gegevens (zie art. 125k en het voorgestelde art. 126m lid 5 en 126t lid 5 Sv). Ik acht het onder omstandigheden gerechtvaardigd een daartoe strekkend bevel te richten tot de verdachte. Het blijkt namelijk in de praktijk dat het bij het toenemend gebruik door criminelen van informatietechnologie voor de politie soms zeer moeilijk, zo niet onmogelijk is om het overtuigend bewijs van het strafbaar feit te leveren, aangezien dit letterlijk ligt "opgesloten" in een computer. Het gaat dan om strafbare feiten die geen andere sporen achterlaten dan in de vorm van gegevensbestanden, zodat het voor de politie ook niet mogelijk is om langs andere weg achter de benodigde gegevens te komen. Zouden die gegevens bijv. zijn neergelegd in een geschrift, dan zou de politie nog via huiszoeking e.d. kunnen trachten op die geschriften beslag te leggen, maar waar het gaat om computerbestanden stuit het onderzoek af op de versleuteling. In zo'n geval acht ik het gerechtvaardigd dat een bevel tot medewerking ook tot de verdachte kan worden gericht. Teneinde te waarborgen dat zo'n bevel alleen in die omstandigheden wordt gegeven, wordt voorgesteld de bevelsbevoegdheid ten aanzien van de verdachte te beperken tot gevallen waarin "uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid" (art. 125m lid 1, 126m lid 6 en 126t lid 6). Deze zinsnede is ontleend aan art. 195d lid 3 Sv.

Deze benadering is in overeenstemming met de eisen die uit art. 6 EVRM volgen. Recent heeft het Europese Hof voor de rechten van de mens in het Saunders-arrest (EHRM 17 december 1996) een belangrijke nuance aangebracht op het in art. 6 besloten liggende nemo-teneturbeginsel. Het stelde in overweging 69:

> "The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which had an existence independent of the will of the suspect such as, *inter alia*, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing."

Uit deze overweging kan worden afgeleid dat het nemo-teneturbeginsel volgens het Hof hoofdzakelijk ziet op de verklaringsvrijheid en niet op het vragen c.q. eisen van medewerking van de verdachte aan de verkrijging van materiaal dat onafhankelijk van zijn wil bestaat. Achtergrond hiervan is onder andere dat verklaringen die onder dwang zijn verkregen, mogelijk onjuistheden bevatten en minder betrouwbare informatie opleveren. Een dergelijk risico bestaat niet ten aanzien van materiaal op het bestaan waarvan de verdachte geen invloed kan hebben. Dit geldt ook voor de kennis van de versleuteling van gegevensbestanden; dergelijke kennis bestaat bijvoorbeeld uit een algoritme, dat door een computerprogramma wordt gebruikt om gegevens te versleutelen. Hoewel bij de hier voorgestelde verplichting dus wel van de verdachte wordt gevraagd om actief, mondeling of schriftelijk, bepaalde kennis over te dragen, is hier geen sprake van een verplichting om in eigen bewoordingen een oorspronkelijke weergave van bepaalde feiten of gebeurtenissen te geven. Hierbij

dient te worden bedacht dat de voorgestelde medewerkingsverplichting zodanig is geclausuleerd dat ze alleen aan een verdachte mag worden opgelegd indien "uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte". Er moet dus voldoende ander materiaal beschikbaar zijn, dat een ernstige verdenking oplevert die rechtvaardigt dat de betrokken persoon tot medewerking wordt verplicht. Deze eis is geheel in lijn met het Funke-arrest (EHRM 25 februari 1993, Series A no. 256-A).

Los van het specifieke nemo-teneturbeginsel is uiteraard vereist dat de procedure als geheel en de wijze waarop het bewijs is vergaard aan de eis van een fair trial voldoen. Ik meen dat de hierboven geformuleerde clausulering van de medewerkingsplicht van de verdachte hiervoor een waarborg is. Voor de wijze waarop de rechter van deze clausule gebruik zal maken, zal verdere jurisprudentie van het Europese Hof voor de rechten van de mens mede richtinggevend zijn.

De (geclausuleerde) medewerkingsverplichting van de verdachte geldt in het voorstel ook ten aanzien van het aftappen van telecommunicatie. De aard van deze opsporingsbevoegdheid brengt uiteraard mee dat een bevel pas tot de verdachte zal worden gericht zodra het aftappen is beëindigd.

Tot slot wijs ik erop dat de overige categorieën verschoningsgerechtigden - de professionele geheimhouders en de naaste bloed- een aanverwanten van verdachten - uitgezonderd blijven van de medewerkingsplicht. Gelet op de andere ratio van hun verschoningsrecht - hun vertrouwensfunctie resp. de familieband waarin de strafvorderlijke overheid niet behoort in te breken - is dit m.i. gerechtvaardigd.

D. ONDERZOEK VAN E-MAIL (Art. I, onderdeel Ka en Kb, art. II, onderdeel A en E (art. 125n))

12. Onderzoek van e-mail

De status van *e-mail* - elektronische post, dat wil zeggen berichten die via computernetwerken worden verzonden - is recentelijk voorwerp van discussie geweest. Aanleiding voor die discussie waren vragen van de leden van de Tweede Kamer Van Zuijlen en Roethof over het juridische kader van onderzoek door politie en justitie van e-mail. In mijn antwoord op die vragen heb ik gesteld dat onbeveiligde e-mails *naar huidig recht* kunnen worden vergeleken met briefkaarten, zodat voor de kennisneming daarvan door justitie geen bijzondere, aanvullende eisen gelden bovenop de algemene waarborgen die gelden voor de kennisneming door justitie van computergegevens (kamerstukken II 1996/97, Aanh. 1370). Vervolgens werd een voorstel ingediend tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim (kamerstukken 1996/97, 25 443, nrs. 1-2). Voorgesteld wordt om hiervoor in de plaats een recht op vertrouwelijke communicatie in de Grondwet op te nemen. De stelling in de memorie van toelichting bij dat voorstel, dat niet-versleutelde of anderszins beveiligde computerberichten niet onder het recht op vertrouwelijke communicatie vallen, heeft eveneens tot veel commentaar aanleiding gegeven.

Inmiddels heeft de regering in de nota naar aanleiding van het verslag bij het voorstel tot Grondwetswijziging haar standpunt met betrekking tot de bescherming van e-mail verder verduidelijkt. Aangegeven wordt dat onderscheid moet worden gemaakt tussen de fase van het transport van e-mail over een telecommunicatienetwerk en de fase van opslag van e-mail op een computer. In die eerste fase is e-mail als ieder ander telecommunicatieverkeer zonder meer beschermd: er geldt een aftapverbod (art. 139c en - speciaal voor personen werkzaam bij een telecommunicatienetwerk of -dienst - 374bis Sr). In de fase van de opslag is e-mail beschermd indien sprake is van de geobjectiveerde wil van de betrokkene om het bericht vertrouwelijk te houden, blijkend uit een bepaalde hindernis die derden moeten nemen om van de communicatie kennis te kunnen nemen. Als hindernis geldt bijvoorbeeld de afscherming van e-mail door middel

van een password. Ook hier voorziet het Wetboek van Strafrecht reeds in bescherming: als iemand de betrokken hindernis onbevoegdelijk neemt en de e-mail van een ander inziet (bijv. door zonder toestemming het password van die ander te gebruiken) is sprake van computervredebreuk: het opzettelijk wederrechtelijk binnendringen in een deel van een geautomatiseerd werk, met doorbreking van enige beveiliging of met aanneming van een valse hoedanigheid of iets dergelijks (art. 138a Sr).

Op één punt schiet de strafrechtelijke bescherming van opgeslagen e-mail mogelijk tekort. Het is namelijk twijfelachtig of een Internet Service Provider zich schuldig maakt aan computervredebreuk als hij zonder toestemming in de mailboxen van zijn abonnees kijkt. Aangezien die mailboxen zich op een geautomatiseerd werk bevinden dat eigendom is van de provider, is het immers de vraag of gesproken kan worden van *wederrechtelijk* binnendringen in het geautomatiseerd werk door de provider. Om deze reden wordt voorgesteld - conform de toezegging gedaan in de nota naar aanleiding van het verslag bij wetsvoorstel 25 443 - om Internet Service providers te brengen onder de werking van art. 372 Sr. Dit artikel verbiedt de persoon werkzaam bij een openbare instelling van vervoer om een poststuk zonder toestemming te openen.

Tot nu toe ging het over de bescherming van de vertrouwelijkheid van e-mail in horizontale verhoudingen (tussen particulieren onderling). Daarnaast is er de bescherming ten opzichte van de overheid, zoals die in het bijzonder in de normering van strafvorderlijke bevoegdheden gestalte krijgt. Ook hierbij dient te worden onderscheiden tussen het transport van e-mail en de opslag ervan. Wat de opslag van e-mail betreft zijn met name van belang de regels voor het onderzoek van gegevens in geautomatiseerde werken (zie art. 125i e.v. Sv). Mij is gebleken dat deze regels voor wat betreft het onderzoek van e-mail te algemeen zijn gesteld, vergeleken bij de regeling van de inbeslagneming van (stoffelijke) geschriften. In die regeling is namelijk voorzien in een bijzondere positie voor brieven en andere post, met name voor zover ze zijn toevertrouwd aan een instelling van vervoer. Art. 100 Sv (zoals voorgesteld door wetsvoorstel 23 251, herziening van het gerechtelijk vooronderzoek) bepaalt dat de officier van justitie instellingen van vervoer kan bevelen poststukken uit te leveren alleen voor zover zij *klaarblijkelijk* van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, ofwel indien zij klaarblijkelijk het voorwerp van het strafbare feit uitmaken of tot het begaan daarvan gediend hebben. De artikelen 101 lid 2 en 114 lid 2 bepalen vervolgens dat van de inhoud van inbeslaggenomen poststukken, *voor zover ze gesloten zijn,* alleen wordt kennisgenomen met toestemming van de rechter-commissaris en alleen voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd enz. Voor het verkrijgen van inzage in post door justitie gelden dus zwaardere eisen dan voor het onderzoek van voorwerpen en geschriften in het algemeen; met name dient een hogere graad van waarschijnlijkheid ("klaarblijkelijk") te bestaan dat de gezochte gegevens direct relevant zijn voor het onderzoek. Doel van deze eisen is om een extra waarborg te geven voor de vertrouwelijkheid van het postverkeer.

Ik ben van mening dat het gewenst is de eisen die gelden voor het onderzoek van poststukken, door te trekken naar het justitieel onderzoek van e-mail. Dit betekent volgens dit voorstel dat e-mails die door iemand via een computernetwerk naar een ander worden verzonden en die tijdelijk (in afwachting van een initiatief van de geadresseerde) zijn opgeslagen op de computer van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, door justitie slechts kunnen worden ingezien op bevel van de rechter-commissaris en alleen voor zover die e-mails klaarblijkelijk van de verdachte afkomstig zijn, voor hem zijn bestemd of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot die e-mails het strafbare feit is gepleegd. Hiertoe dient o.a. wijziging te worden gebracht in artikel 125i Sv, dat nu een algemene bevoegdheid voor de RC bevat om computergegevens op te vragen.

Met nadruk wijs ik erop dat de hier voorgestelde regeling slechts ziet op e-mail die is opgeslagen op de computer van de serviceprovider van de verzender of de geadresseerde,

beschikbaar om door de betrokkene langs elektronische weg te worden "gedownload". Teneinde inzage te verkrijgen in die post zal justitie de weg moeten kiezen van huiszoeking bij bijv. de provider of een bevel tot uitlevering van gegevens op grond van artikel 125i Sv. In dat geval gelden de hier voorgestelde beperkingen (bevel van de r-c en alleen post klaarblijkelijk van de verdachte afkomstig, voor hem bestemd enz.). Anders ligt het wanneer justitie e-mail in de fase van het transport wil onderscheppen. Hier is geen sprake van opgeslagen, reeds bestaande gegevens, maar van toekomstige, nog niet bestaande gegevens. Daarvoor staat niet de weg open van artikel 125i, maar die van artikel 125g (het aftappen van telecommunicatie, art. 126m en 126t volgens wetsvoorstel 25 403). Ook eerdergenoemde Aanbeveling Nr. R (95) 13 van de Raad van Europa betreffende problemen van strafprocesrecht in verband met informatietechnologie maakt een duidelijk onderscheid tussen het strafvorderlijke onderzoek van gegevens opgeslagen in een computer enerzijds en het onderzoek (i.c. het onderscheppen) van gegevens tijdens hun transport. Uitgangspunt nr. 1 van de Aanbeveling schrijft voor dit onderscheid duidelijk in de wetgeving tot uitdrukking te brengen. Mede hierom wordt voorgesteld de bevoegdheid van artikel 125i Sv uitdrukkelijk te beperken tot gegevens "die zijn opgeslagen in een geautomatiseerd werk". De huidige omschrijving ("gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk") roept bij sommigen het misverstand op dat art. 125i ook zou zien op toekomstige, nog niet bestaande gegevens.

E. OPSPORINGSONDERZOEK OP OPENBARE COMPUTERNETWERKEN (Art. II, onderdeel G en I)

13. Inleiding

Met de opkomst van openbare computernetwerken zoals Internet is de vraag actueel geworden wat opsporingsambtenaren op deze netwerken vermogen. In het bijzonder rijst de vraag of de bestaande opsporingsbevoegdheden, alsmede de in wetsvoorstel 25 403 voorgestelde bijzondere opsporingsbevoegdheden op Internet kunnen en mogen worden uitgeoefend, dan wel aanpassing behoeven.

Onderscheid dient te worden gemaakt tussen het rondkijken op een netwerk voor zover dat voor het publiek toegankelijk is en het verrichten van (opsporings)handelingen op zo'n netwerk waarbij inbreuk wordt gemaakt op de (grond)rechten van burgers. Wat het eerste betreft staat niets de politie in de weg om een contract te sluiten met een provider teneinde een aansluiting te verkrijgen op Internet. Vervolgens kunnen politie-ambtenaren als ieder ander rondkijken in de digitale wereld en kennis nemen van de voor een ieder raadpleegbare informatie. Daarvoor is niet vereist dat zij een verdenking van een strafbaar feit hebben. Evenmin behoeven zij hun hoedanigheid van opsporingsambtenaar bekend te maken. Zoals de politie, al dan niet in burger, op straat mag surveilleren en rondkijken, zo mag een rechercheur vanachter zijn computer hetzelfde doen op Internet. Een uitdrukkelijke wettelijke grondslag is daarvoor niet nodig, mits dat optreden gerekend kan worden tot de uitvoering van de politietaak (zie art. 2 Politiewet 1993).

Een en ander geldt m.i. ook voor Internetsites die aan opsporingsambtenaren de toegang ontzeggen ("Stop! Are you a law enforcement agent?"). Beheerders van dergelijke sites kunnen redelijkerwijs niet de verwachting hebben dat, waar zo'n site voor ieder ander toegankelijk is en dus feitelijk een openbaar karakter draagt, alleen opsporingsambtenaren zich van kennisneming zullen onthouden. Opsporingsambtenaren behoeven zich in zo'n geval dan ook niet aan het toegangsverbod te storen. Evenmin behoeven zij zich onder hun werkelijke naam bekend te maken. Op Internet is het immers geenszins ongebruikelijk om anoniem of onde een pseudoniem te "surfen". Onder deze omstandigheden kan het gebruik door een opsporingsambtenaar van een pseudoniem niet als misleiding van andere gebruikers van Internet worden aangemerkt. Anders

wordt het overigens wanneer het onderzoek in en naar zo'n site een stelselmatig karakter krijgt (zie de volgende paragraaf).

De bevoegdheid om rond te kijken op een openbaar netwerk impliceert nog niet de bevoegdheid om stelselmatig voor de uitoefening van de politietaak gegevens omtrent onverdachte personen van Internet te downloaden en in een politieregister op te slaan. Hierbij is niet relevant of het gaat om gegevens die zijn verkregen door deelname aan newsgroups of ontleend aan op Internet voor ieder toegankelijke bestanden. Dergelijke gegevens mogen blijkens artikel 4 van de Wet politieregisters immers slechts worden opgeslagen voor de uitoefening van de politietaak. Dit laat onverlet dat voor de opsporing van een bepaald strafbaar feit uiteenlopende persoonsgegevens van Internet worden gedownload en worden opgenomen in een tijdelijk register in de zin van deze wet, teneinde vervolgens te kunnen worden geanalyseerd en in verband gebracht met andere gegevens.

Tegenover het rondkijken op een openbaar netwerk staat het op zo'n netwerk verrichten van opsporingshandelingen waarbij inbreuk wordt gemaakt op de rechten van burgers. Daartoe zijn politie en justitie alleen bevoegd indien daarvoor een uitdrukkelijke wettelijke grondslag bestaat. Veel van de bestaande wettelijke opsporingsbevoegdheden zijn op een computernetwerk naar hun aard niet toepasbaar omdat toepassing alleen aan de orde kan zijn bij de fysieke aanwezigheid van personen of goederen, zoals de aanhouding van verdachten of de inbeslagneming van voorwerpen. Andere bevoegdheden daarentegen kunnen op een netwerk wel degelijk relevant zijn. Ik wijs op de in dit wetsvoorstel voorgestelde bevoegdheden tot ontoegankelijkmaking en vernietiging van bepaalde gegevens - de desbetreffende bepalingen maken geen onderscheid tussen een *stand alone* computer en een computer die is verbonden met een netwerk, zodat ze ook op een netwerk toepasbaar zijn -, alsmede op bijzondere opsporingsbevoegdheden zoals infiltratie en observatie, die thans nog op ongeschreven recht zijn gebaseerd maar door wetsvoorstel 25 403 van een wettelijke basis worden voorzien. Uitgangspunt bij dit soort bevoegdheden (die dus niet noodzakelijk betrekking hebben op fysiek aanwezige personen of goederen) dient mijns inziens te zijn dat ze, naast de "normale" toepassing in de fysieke wereld, ook toepasbaar moeten zijn in de "digitale wereld". Daarbij dienen dezelfde voorwaarden te gelden als voor de normale toepassing, tenzij de specifieke aard van het onderzoek in een geautomatiseerde omgeving om specifieke voorzieningen vraagt. In de volgende paragraaf zullen enkele bijzondere opsporingsbevoegdheden aan dit uitgangspunt worden getoetst.

Bij het voorgaande dient een belangrijk voorbehoud te worden gemaakt. Nederlandse opsporingsambtenaren mogen op computernetwerken slechts onderzoek doen voor zover de Nederlandse rechtsmacht reikt. Dit betekent dat zij geen onderzoek mogen doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden of wanneer er zodanige aanwijzingen zijn dat er een gerede kans is dit het geval is. Aangenomen mag worden dat dit slechts uitzondering lijdt voor zover de opsporingsambtenaar, zoals hierboven aangegeven, als ieder ander mag rondkijken op een openbaar netwerk. Het staat een opsporingsambtenaar dus vrij om met sites waarvan de databestanden zijn opgeslagen op buitenlandse computers, een verbinding te leggen teneinde die sites te bekijken. Wat de opsporingsambtenaar echter níet mag, is op die sites bevoegdheden uitoefenen waarbij inbreuk wordt gemaakt op de rechten van burgers. Voor de voorgestelde maatregel van ontoegankelijkmaking van gegevens betekent dit bijvoorbeeld dat hij niet mag worden toegepast ten aanzien van gegevens waarvan men redelijkerwijs kan vermoeden dat zij zijn opgeslagen in een buitenlandse computer en zich dus aan de Nederlandse rechtsmacht onttrekken. Indien de maatregel op goede gronden wordt toegepast, maar later blijkt dat, anders dan redelijkerwijs kon worden vermoed, de maatregel *de facto* in een computer in het buitenland heeft plaatsgevonden, moet onmiddellijk contact worden opgenomen met de autoriteit van het desbetreffende land teneinde in onderling overleg te bezien wat te doen. Denkbaar is overigens dat met andere landen afspraken worden gemaakt om in zo'n geval het land dat wel bevoegd is, te waarschuwen opdat het de maatregel van Nederland kan overnemen. Internationaal overleg over dit soort wederzijdse rechtshulp is recentelijk van start gegaan, onder andere in het kader van de Raad

van Europa. Het Comité van Ministers heeft in 1996 opdracht gegeven een daartoe strekkend verdrag te ontwerpen. Het is verheugend dat onder meer vertegenwoordigers van de Verenigde Staten en Canada alsmede van de UNESCO aan de beraadslagingen deelnemen. Het moge duidelijk zijn dat internationaal overleg dringend noodzakelijk is om de problemen die het grenzeloze karakter van Internet voor de opsporing van strafbare feiten meebrengt, het hoofd te kunnen bieden.

14. Bijzondere opsporingsbevoegdheden; pseudokoop

In de memorie van toelichting bij het wetsvoorstel Bijzondere opsporingsbevoegdheden (kamerstukken II 1996/97, 25 403, nr. 3) wordt op verschillende plaatsen ingegaan op de toepasbaarheid van de voorgestelde bevoegdheden op een openbaar computernetwerk zoals Internet. Zo is daarin aangegeven dat infiltratie - het door een opsporingsambtenaar deelnemen of medewerking verlenen aan een groep van personen waarbinnen naar redelijkerwijs kan worden vermoed misdrijven worden beraamd of gepleegd (zie de voorgestelde artt. 126h en 126p Sv) - ook mogelijk is op Internet (memorie van toelichting, a.w., p. 29). Daarbij is als voorbeeld gegeven de infiltratie in een netwerk van personen dat via Internet kinderporno distribueert, waarbij de opsporingsambtenaar zich (ook) op het net dient te begeven. Kenmerkend voor infiltratie is dat wordt meegewerkt of deelgenomen aan een criminele groep, zodat het risico bestaat dat de betrokken opsporingsambtenaar strafbare feiten moet plegen, terwijl de andere deelnemers worden misleid omtrent de werkelijke motieven van de infiltrant. Gelet op dit (ingrijpende) karakter is de bevoegdheid aan strikte voorwaarden gebonden (o.a. is een bevel van de officier van justitie vereist). Aan deze voorwaarden zal ook bij optreden op Internet moeten worden voldaan.

Mutatis mutandis geldt hetzelfde voor het zgn. stelselmatig inwinnen van informatie over de verdachte, zonder dat de opsporingsambtenaar als zodanig kenbaar is (zie het voorgestelde art. 126j Sv). Denkbaar is dat dit de vorm aanneemt van het stelselmatig deelnemen aan een newsgroup op Internet waaraan ook de verdachte deelneemt, zonder dat de deelnemers aan de newsgroup weten dat zich onder hen een opsporingsambtenaar bevindt (memorie van toelichting, a.w., p. 34). Deze bevoegdheid onderscheidt zich van infiltratie doordat niet wordt deelgenomen aan een groep van personen waarbinnen misdrijven worden beraamd of gepleegd. Kenmerkend is verder dat sprake is van een stelselmatig onderzoek; alleen in geval van stelselmatigheid kan worden gesproken van een inbreuk op de persoonlijke levenssfeer van de verdachte die een aparte wettelijke grondslag behoeft. Zoals in de vorige paragraaf aangegeven levert daarentegen het eenmalig anoniem door een politie-ambtenaar deelnemen aan een newsgroup niet een dergelijke inbreuk op de privacy van de verdachte op, zodat daarvoor niet de voorwaarden van het voorgestelde artikel 126j gelden.

Een andere bevoegdheid uit wetsvoorstel 25 403 blijkt niet geschikt voor toepassing op een computernetwerk, waar dit wel wenselijk is. Het betreft de bevoegdheid tot pseudo-koop en pseudo-dienstverlening, dat wil zeggen het in het belang van het onderzoek door een opsporingsambtenaar goederen afnemen van of diensten verlenen aan de verdachte (zie de voorgestelde artt. 126i en 126q Sv). Hierbij is met name gedacht aan fysieke handelingen zoals het afnemen van drugs en het verlenen van transportdiensten. Op Internet zijn echter opsporingshandelingen denkbaar die erg op de genoemde lijken en dezelfde strekking hebben, maar niettemin niet onder de thans voorgestelde bepalingen kunnen worden gebracht. Ik doel hier op onderzoek naar de handel op Internet in illegale uitingen of programmatuur (bijv. illegale software, kinderporno). Het kan daarbij wenselijk zijn dat een politie-ambtenaar op een bepaalde aanbieding ingaat en de betrokken gegevens afneemt. In de praktijk is gebleken dat aan een daartoe strekkende bevoegdheid behoefte bestaat. Ook het in de vorige paragraaf genoemde uitgangspunt dat wat in de fysieke wereld ter opsporing mogelijk is, in de digitale wereld ook mogelijk moet zijn, rechtvaardigt een aanpassing van de pseudekoopbepalingen. Ik stel dan ook voor in de door wetsvoorstel 25 403 voorgestelde artikelen 126i en 126q op te nemen dat de officier van justitie in het belang van het onderzoek kan bevelen

dat een opsporingsambtenaar "*gegevens afkomstig uit een geautomatiseerd werk door tussenkomst van een openbaar telecommunicatienetwerk afneemt van de verdachte*". In genoemd wetsvoorstel is ook de zgn. burgerpseudo-koop geregeld, dat wil zeggen de bijstandverlening aan de opsporing door een gewone burger bestaande uit het door deze afnemen van goederen van of het verlenen van diensten aan de verdachte (artt. 126ij en 126z Sv). Ik heb ervan afgezien om ook deze bepalingen aan te passen aan de opsporing in een openbaar computernetwerk, aangezien de tussenkomst van een netwerk het de politie mogelijk maakt om de pseudokoop altijd zelf uit te voeren.

15. Handhaving

Over de uitvoerbaarheid en handhaafbaarheid van het hier voorgestelde merk ik het volgende op. In het wetsvoorstel worden geen nieuwe gedragingen strafbaar gesteld (met uitzondering van het voorgestelde art. 372, tweede lid, Sr). Wel wordt voorzien in een uitbreiding van het instrumentarium voor de opsporing en vervolging van criminaliteit waarbij de moderne informatie- en telecommunicatietechnologie een rol speelt (vgl. de voorgestelde ontoegankelijkmaking van gegevens, de medewerkingsverplichting t.a.v. de ontsleuteling van gegevens en de aangepaste pseudekoopbevoegdheid t.b.v. het onderzoek op een openbaar computernetwerk). Daarnaast worden waarborgen gegeven voor een behoorlijk overheidsoptreden, met inachtneming van de (grond)rechten van de burgers (vgl. de beperking van de aansprakelijkheid van tussenpersonen en de nadere regulering van het onderzoek van e-mail). Ik verwacht dat al deze voorstellen tezamen zullen bijdragen aan een adequate aanpak - en waar nodig een verbetering daarvan - van criminaliteit in een geautomatiseerde omgeving, bijvoorbeeld op Internet. Over de effectiviteit van de voorstellen zijn geen ondubbelzinnige uitspraken te doen. Ten eerste is dat niet mogelijk omdat het totale aantal strafbare feiten of opsporingsonderzoeken waarvoor de onderhavige voorstellen mogelijk relevant zijn, niet of nauwelijks is vast te stellen of te schatten. Door de snelle verbreiding van het gebruik van moderne informatietechnologie (computers, GSM-telefoons, satellietcommunicatie, elektronische agenda's) speelt die technologie tegenwoordig immers ook bij traditionele criminaliteit vaak een rol. Verder geldt voor de uitings- en verspreidingsdelicten die worden gepleegd via een computernetwerk als Internet, dat de omvang en ernst van het probleem niet op zinvolle wijze per land is vast te stellen vanwege het grensoverschrijdende (zelfs wereldomspannende) karakter van deze delicten.

Naast een toereikend wettelijk instrumentarium vormen een adequate organisatie, goed opgeleide politie- en justitiefunctionarissen alsmede de beschikbaarheid van een kwalitatief hoogwaardige informatietechnologische uitrusting noodzakelijke voorwaarden voor een goede strafrechtelijke rechtshandhaving op de elektronische snelweg. De opbouw van de organisatie van de handhaving - inclusief de personele en materiële middelen - is momenteel in volle gang. De regionale politiekorpsen hebben inmiddels vijf interregionale teams computercriminaliteit opgezet, die - in samenwerking met de CRI en de Afdeling Computeronderzoek van het Gerechtelijk Laboratorium - ondersteuning verlenen bij opsporingsonderzoeken waarbij informatietechnologie een rol speelt. Van belang is dat binnen de politie en justitie bestaande hiaten in de kennis van deze technologie door middel van bijscholing worden verholpen. Over de voornemens op het gebied van organisatie, opleiding en uitrusting zal de Tweede Kamer naar verwachting voor het zomerreces van 1998 nader worden geïnformeerd.

De voorstellen brengen voor de burger slechts beperkte lasten mee. Zoals aangegeven wordt de strafrechtelijke aansprakelijkheid van tussenpersonen die beroeps- of bedrijfsmatig informatie doorgeven, beperkt. In het algemeen is voldoende dat zij, zodra zij op de hoogte komen of een vermoeden krijgen van de aanwezigheid van strafbaar materiaal, adequate maatregelen nemen ter voorkoming van verdere verspreiding van dat materiaal. Stelselmatig, preventief onderzoek wordt van tussenpersonen niet geëist. Deze regeling sluit goed aan bij reeds bestaande vormen van

zelfregulering van de Internet Service Providers op het terrein van kinderporno en racisme (vgl. Evaluatie Internet Meldpunt Kinderporno, Stichting meldpunt ter bestrijding van kinderpornografie op het Internet, Amsterdam 1997). Adequate zelfregulering kan ertoe leiden dat niet naar het middel van het strafrecht behoeft te worden gegrepen.

Ook de voorgestelde verplichting voor o.a. aanbieders van telecommunicatienetwerken en -diensten om mee te werken aan het ontsluieren van gegevensverkeer brengt voor de burger geen grote lasten mee. Hierop is in par. 10 aan het slot reeds ingegaan.

16. Artikelsgewijze toelichting

Naast de hierboven toegelichte voorstellen wordt een groot aantal minder ingrijpende wijzigingen voorgesteld van bestaande, bij de eerste Wet computercriminaliteit ingevoerde bepalingen. Het betreft art. I, onderdeel C t/m Kb, en art. II, onderdeel A, B, C en F.

Artikel I

A

Dit onderdeel bevat de wijziging van de regeling van de uitgeversaansprakelijkheid zoals neergelegd in artikel 53 Sr. Aan dit onderwerp werd in het algemeen deel, onderdeel A, reeds een algemene beschouwing gegeven.

De bescherming tegen strafrechtelijke vervolging die art. 53 Sr aan de tussenpersoon verleent, wordt uitgebreid tot alle "uitingen in gesproken woord, beeld of geschrift". Gezocht is naar een moderne omschrijving, die niet is gekoppeld aan de gebruikte techniek. Onder "uitingen in gesproken woord" moeten bijvoorbeeld niet alleen worden verstaan de woorden afkomstig uit de mond van personen, maar ook "computerspeak". Overigens is het niet de bedoeling met deze omschrijving de betekenis van in bestaande delictsomschrijvingen voorkomende begrippen als "geschrift" of "mondelinge uitlating" te beperken.

De kern van de voorgestelde wijziging is de vervanging van de uitgever door de professionele tussenpersoon die informatie afkomstig van derden openbaar maakt of verspreidt. Ik ga op drie kenmerken van het begrip "tussenpersoon" nader in: 1. het beroepsmatig handelen, 2. het vermenigvuldigen ten behoeve van het publiek en 3. de intermediaire rol.

Ad 1. De "tussenpersoon" maakt zijn beroep of bedrijf van de openbaarmaking of verspreiding van informatie van derden aan derden. Een ieder kan zich tot de tussenpersoon wenden om voor hem informatie te verspreiden. Het moet daarbij gaan om een hoofdwerkzaamheid van de (tussen)persoon, zij het wellicht een naast andere werkzaamheden. Speelt de verspreiding van informatie in het geheel van de werkzaamheden slechts een ondergeschikte rol, staat zij ten dienste van een andere werkzaamheid, dan is geen sprake van een professionele tussenpersoon. Een reclame- of *public relations* bureau, bijvoorbeeld, zal wellicht geschriften of afbeeldingen afkomstig van een cliÎnt onder het publiek verspreiden, maar dit is geen zelfstandige werkzaamheid van het bureau, maar staat ten dienste van de hoofdtaak: het bevorderen van de bekendheid en externe relaties van die cliÎnt.

Ad 2. De professionele tussenpersoon maakt informatie openbaar, verspreidt informatie. Dit wil zeggen dat hij de informatie voor het publiek beschikbaar maakt. Van openbaarmaking of verspreiding is geen sprake als de informatie slechts voor een of enkele bijzondere personen bestemd is; de informatie moet algemeen, voor een grotere groep mensen toegankelijk zijn. Een telefoonbedrijf kan niet gezegd worden informatie openbaar te maken of te verspreiden. Het verzorgt in de regel slechts de communicatie tussen twee of meer (vgl. telefonisch vergaderen) bepaalde personen. Dit neemt niet weg dat hetzelfde bedrijf ook andere, zelfstandige diensten kan

aanbieden die wel bestaan uit de verspreiding van informatie onder het publiek, en in zoverre wèl onder de bescherming van artikel 53 Sr valt.
Ad 3. Het gaat bij de informatieverspreiding door de tussenpersoon om uitingen *afkomstig van derden*. De verspreiding van informatie waarvan de verspreider geheel of grotendeels zelf de bron is, valt niet onder de bescherming van artikel 53 Sr. De professionele tussenpersoon geeft informatie door. Hij is, zoals minister Modderman het indertijd noemde toen hij over de uitgever sprak, slechts technisch instrument. Dit betekent dat de informatie in min of meer onbewerkte staat aan het publiek wordt aangeboden. Een journalist kan dan ook niet als een professionele tussenpersoon worden beschouwd: weliswaar is zijn informatie grotendeels afkomstig van derden, maar voordat hij die informatie publiek maakt, bewerkt, becommentarieert, selecteert en combineert hij. Ook degeen die een bloemlezing verzorgt is geen tussenpersoon, omdat in de selectie een pesoonlijke inbreng aanwezig is.

In de eerste voorwaarde voor niet-vervolgbaarheid is een kleine wijziging aangebracht: de eis dat de tussenpersoon zijn "naam en woonplaats" bekendmaakt is vervangen door de eis dat hij zijn "identiteit" bekendmaakt. Reden hiervoor is dat het technisch niet altijd eenvoudig is naam en woonplaats bekend te maken (bijv. op Internet). Wel dient de opgave van de tussenpersoon zodanig te zijn dat zij politie en justitie in staat stelt om - zonder onevenredige inspanning - langs andere weg de naam en woonplaats van de tussenpersoon te achterhalen.

De tweede voorwaarde (betreffende het noemen van de "dader") vereist dat de tussenpersoon degene noemt die het feit heeft gepleegd (dat wil zeggen alle bestanddelen van de delictsomschrijving heeft vervuld), heeft doen plegen, heeft medegepleegd of opzettelijk heeft uitgelokt (zie art. 47 lid 1 Sr). Het gaat met andere woorden om het noemen van een persoon die voor een belangrijk deel als bron of oorzaak van de strafbare uiting kan worden aangemerkt. Vaak zal dit de auteur zijn. Niet voldoende is dus dat de tussenpersoon een andere tussenpersoon noemt die als vorige schakel een rol heeft gespeeld bij de verspreiding of openbaarmaking van de betrokken strafbare informatie.

B

Omdat drukkers, voor zover zij zich beperken tot hun eigenlijke werk en niet zelf ook de gedrukte werken verspreiden, niet vallen onder het begrip "tussenpersoon", dient artikel 54 te worden gehandhaafd. De thans in het tweede lid neergelegde "grijpbaarheidsvoorwaarde" - de hoofddader dient vervolgbaar te zijn en zich in Nederland te bevinden - is echter ook met betrekking tot het drukkerswerk achterhaald door de internationalisering. Zij wordt dan ook, conform de wijziging van artikel 53, geherformuleerd en overgebracht naar het eerste en nu enige lid. Zie verder par. 5 van het algemeen deel.

C

Dit betreft een correctie van de eerste Wet computercriminaliteit. Zij is mede ingegeven door een bespreking van prof. Kaspersen van deze wet (De Wet computercriminaliteit is er - nu de boeven nog, Computerrecht 1993/4, blz. 134 e.v.). De woorden "*al dan niet* op een overeengekomen wijze" in de definitie van het begrip "gegevens" zijn in feite zinledig. Gegevens krijgen hun betekenis door een onderliggende afspraak. Theoretisch is weliswaar denkbaar dat een computer wordt ontwikkeld die over een coderingssysteem beschikt dat op geen enkele wijze gegevens kan uitwisselen met andere computers - een computer met andere woorden die uitsluitend geschikt is voor het gebruik door één enkel persoon -, maar deze mogelijkheid mist maatschappelijke relevantie, zodat de woorden "al dan niet" in art. 80quinquies kunnen worden gemist.

D, E en F, onderdeel 1

Dit onderdeel beoogt aan de definitie van een geautomatiseerd werk de overdrachtsfunctie toe te voegen. Deze functie is een wezenskenmerk van een geautomatiseerd werk, dat immers met name bestemd is om daarin opgeslagen of verwerkte gegevens aan de gebruiker terug te geven of aan een ander (computer-)systeem over te dragen.

De definitie spreekt van opslag, verwerking èn overdracht van gegevens. Het gaat hier om cumulatieve voorwaarden. Een inrichting die enkel bestemd is om gegevens over te dragen (een eenvoudig telefoontoestel, bepaalde zend- en ontvanginrichtingen) of op te slaan valt dus buiten de begripsomschrijving.

Enkele strafbepalingen spreken nog van geautomatiseerde werken "voor (de) opslag of verwerking van gegevens". Gelet op de definitie in de betekenistitel van het wetboek is deze specificatie overbodig en kan ze dan ook worden geschrapt (E, F, onderdeel 1).

F

Artikel 138a Sr (computervredebreuk) wordt op twee punten gewijzigd. In het eerste lid wordt tussen de woorden "opzettelijk wederrechtelijk" het woordje "en" opgenomen. Dit betekent dat niet meer bewezen behoeft te worden dat de verdachte wist dat zijn handelen wederrechtelijk was. Dit is een onnodig zware eis: bij iemand die een beveiliging doorbreekt of de toegang verwerft door een technische ingreep o.i.d., mag wetenschap van het wederrechtelijke van zijn handelen worden verondersteld, behoudens natuurlijk een beroep op verontschuldigbare rechtsdwaling.

De schrapping van de woorden "voor de opslag of verwerking van gegevens" - een overbodige specificatie van "geautomatiseerd werk" - is hierboven reeds toegelicht.

Het derde lid bevat twee gekwalificeerde vormen van computervredebreuk. Die onder a betreft het gebruik maken van de verwerkingscapaciteit van het geautomatiseerd werk waarin betrokkene is binnengedrongen. Voorgesteld wordt om het bestanddeel "met het oogmerk om zich wederrechtelijk te bevoordelen" aan te vullen met het oogmerk om *een ander* te bevoordelen. Overigens zijn de gekwalificeerde strafbepalingen van het derde lid alleen van toepassing indien de computervredebreuk heeft plaatsgevonden door tussenkomst van een openbaar telecommunicatienetwerk. Ratio hiervan is dat de strafverzwaring vooral wordt gerechtvaardigd doordat gebruik is gemaakt van de anonimiteit van een dergelijk netwerk, waardoor de opsporing aanzienlijk wordt bemoeilijkt.

G

Deze wijziging betreft een tekstuele verduidelijking van artikel 139b, tweede lid, Sr. Over de betekenis van dit artikel merk ik het volgende op.

De artikelen 139a tot en met 139c Sr stellen het met een technisch hulpmiddel afluisteren, aftappen of opnemen van gesprekken en ander gegevensverkeer strafbaar. Artikel 139b betreft het gegevensverkeer elders dan in een woning, besloten lokaal of erf. Het eerste lid ziet op het afluisteren van gesprekken, het tweede lid op het aftappen van gegevensoverdracht door middel van een geautomatiseerd werk of door middel van telecommunicatie. Met het aftappen van gegevensoverdracht door middel van een geautomatiseerd werk wordt gedoeld op het aftappen van de zgn. residustraling van een computerscherm. Dit is mogelijk met bepaalde gevoelige apparatuur, die is geplaatst in de nabijheid (zij het soms daarvan gescheiden door een muur) van het beeldscherm dat de straling genereert.

Verder is afzonderlijk strafbaar het aftappen of opnemen van gegevensoverdracht door middel van telecommunicatie via een kabel of via de ether. Hiermee wordt in het kader van artikel 139b, tweede lid, bedoeld de telecommunicatie anders dan via een *openbaar*

telecommunicatienetwerk; daarop ziet immers artikel 139c (zie ook art. 139b, derde lid, in verband met art. 139a, derde lid, onder 1). Hierbij moet met name worden gedacht aan telecommunicatie via een bedrijfsnetwerk. Ook het aftappen daarvan is dus strafbaar, tenzij - wat het aftappen van telecommunicatie via de ether betreft - voor het aftappen geen bijzondere inspanning behoeft te worden geleverd. Deze laatste beperking volgt uit artikel 139c, tweede lid, onder 1, waarnaar art. 139b (derde lid) verwijst. Zij vindt haar rechtvaardiging in het feit dat bij telecommunicatie degenen die met elkaar communiceren, zich niet in elkaars nabijheid bevinden en dus welbewust gegevens over een afstand verzenden. Voor zover de gegevens zonder bijzondere inspanning kunnen worden onderschept, dienen betrokkenen daarmee rekening te houden en kan van strafbaar aftappen geen sprake zijn.

Tussen de woorden "opzettelijk" en "zonder daartoe gerechtigd te zijn" wordt het woordje "en" geplaatst. Daarvoor geldt dezelfde reden als bij artikel 138a, eerste lid (zie onderdeel F).

H

(vervallen)

I

Dit onderdeel betreft een verduidelijking van de begrippen "betaalpas" en "waardekaart" in het valsheidsdelict van artikel 232 Sr. Er komen steeds meer verschillende kaarten op de markt met soms verschillende functies. Betaling in financiële zin is al lang niet meer de enige functie van dit soort kaarten (vgl. de telefoonkaart of de SIM-kaart voor GSM-telefonie). Hoewel "betalingen" in artikel 232 ook in de ruimere betekenis van "prestaties" kan worden opgevat, wordt voorgesteld ook het verrichten van andere prestaties dan financiële betalingen als mogelijke bestemming van dit soort kaarten op te nemen. Ook wordt opgenomen de bestemming tot het *verkrijgen* van betalingen of andere prestaties. Een waardekaart bijvoorbeeld is vaak bij verkrijging reeds betaald en dient in dat geval dus enkel nog tot het verkrijgen van de tegenprestatie van de uitgever van de kaart (vgl. de telefoonkaart).

De hier voorgestelde omschrijving sluit aan bij de maatschappelijke functie van betaalpassen en waardekaarten. Daarnaast hebben ze in juridisch-technische zin de bestemming om tot bewijs te dienen van het gebruiksrecht van hun houder met betrekking tot een bepaald geautomatiseerd systeem. Dit rechtvaardigt ook de plaatsing van artikel 232 in de titel over valsheid in geschrift.

De wijziging van het tweede lid is van louter terminologische aard.

J en K

Teneinde het misverstand te voorkomen dat de strafbepaling van artikel 350a ook zou zien op de situatie dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen of worden verwerkt, elders - buiten dat werk - worden beschadigd (bijv. wanneer ze op een losse floppy zijn opgeslagen), is de bepaling verduidelijkt. De beschadiging van externe gegevensdragers valt derhalve niet onder het bereik van deze bepaling. Artikel 350b is dienovereenkomstig aangepast (onderdeel J, onder 1, en onderdeel K onder 1).

In onderdeel J, onder 2, wordt het bepaalde in artikel 350a, derde lid, aangescherpt en ruimer geformuleerd. Aangescherpt omdat de zinsnede "bedoeld zijn om schade aan te richten" is gewijzigd in: bestemd zijn om schade aan te richten. Het woord "bestemd" is nauwkeuriger en toont zowel de bedoeling van de dader als de geschiktheid van het middel.

Verder is "door zichzelf te vermenigvuldigen" als zijnde te beperkend vervallen. Behalve door gegevens die schadelijk zijn door hun vermenigvuldiging in een geautomatiseerd systeem kan immers ook schade aan een systeem worden toegebracht door programma's die een of meer

systeemfuncties uitvoeren, waardoor bij voorbeeld de gegevens op het externe geheugen verloren gaan of het systeem vastloopt. Ook het ter beschikking stellen of verspreiden van zgn. logische bommen en trojaanse paarden valt met deze wijziging onder het bereik van artikel 350a, derde lid. De culpose variant van deze strafbepaling is in overeenkomstige zin aangepast (onderdeel K onder 2).

Ka en Kb

De aanvulling van artikel 372 Sr voorziet in strafrechtelijke sanctionering van het verbod voor Internet Service Providers om zonder toestemming van een abonnee inzage te nemen in e-mails die bestemd zijn voor of afkomstig zijn van die abonnee en die (tijdelijk) zijn opgeslagen in een e-mailbox op de computer van de provider. Zie par. 12 van het algemeen deel. Deze aanvulling maakt ook een wijziging van artikel 371 Sr nodig, dat ziet op de ambtenaar die, met overschrijding van zijn bevoegdheid, een persoon die werkzaam is bij de PTT of een andere instelling voor telecommunicatie ertoe brengt een aan die instelling toevertrouwde brief of ander bericht over te leggen.
Strikt genomen betreft het nieuwe artikel 372, tweede lid, geen ambtsdelict, omdat een persoon die werkzaam is bij bijvoorbeeld een Internet Service Provider geen ambtenaar is. Niettemin is plaatsing bij de "echte" ambtsdelicten met betrekking tot post en telecommunicatie gerechtvaardigd, aangezien de werkzaamheid van een Internet Service Provider een vergelijkbare publieke nutsfunctie betreft. Om dezelfde reden werden bij de privatisering van de PTT de betrokken ambtsdelicten gehandhaafd en uitgebreid tot "een persoon werkzaam bij enige openbare instelling van vervoer" (Wet van 26 oktober 1988, Stb. 521).

L en M

Artikel 418 Sr is in zekere zin het spiegelbeeld van artikel 53 Sr: als aan een van de voorwaarden voor uitsluiting van vervolging niet is voldaan, is de tussenpersoon *als zodanig* strafbaar wegens de openbaarmaking of verspreiding van strafbare informatie. Verwezen zij verder, voor wat betreft de eis dat sprake moet zijn van verwijtbaarheid van de tussenpersoon, naar paragraaf 6.

De clausule "tenzij op deze persoon het bij of krachtens de Mediawet bepaalde van toepassing is" strekt ertoe te voorkomen dat het strafrecht het bestuursrechtelijke regime van de Mediawet doorkruist. De Mediawet voorziet in een stelsel van vergunningen ("concessies"), rechten en verplichtingen van de media (in het bijzonder omroepverenigingen en -instellingen) en faciliterende personen (zoals beheerders van draadomroepinrichtingen), inclusief een stelsel van toezicht en eventuele sancties. Het stelsel van de Mediawet brengt mee dat op het terrein van die wet het bestuursrechtelijk toezicht voorop staat en het strafrecht in beginsel geen rol speelt. Om deze reden is het wenselijk de personen op wie dit stelsel van toepassing is, buiten het bereik van de aparte strafbaarstelling van tussenpersonen te laten. Zij kunnen in voorkomend geval uiteraard wel profiteren van de vervolgingsuitsluitingsgrond van artikel 53 Sr. Wat de uitgevers van persorganen betreft (zie hfd. IX van de Mediawet) dient wel te worden opgemerkt dat zij alleen buiten de definitie van "tussenpersoon" in de zin van artikel 418 Sr vallen als zij daadwerkelijk onder het regime van de Mediawet vallen, d.w.z. steun ontvangen van het Bedrijfsfonds voor de pers.

De aparte strafbaarstelling van de drukker, neergelegd in artikel 419 Sr, is gehandhaafd, zij het dat de voorwaarde dat de drukker wist of moest verwachten dat zijn opdrachtgever niet vervolgbaar of buiten Nederland gevestigd zou zijn, daaruit is verdwenen en vervangen door de nieuwe voorwaarde dat hij op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, heeft nagelaten alle handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van de openbaarmaking of verspreiding.

Artikel II

A

De schrapping in art. 125i lid 1 van de woorden "worden verwerkt of overgedragen met gebruikmaking" (van een geautomatiseerd werk) is reeds in paragraaf 12 toegelicht. De overige wijzigingen in de formulering van de eerste twee leden van artikel 125i betreffen correcties van taalkundige aard, voorgesteld naar aanleiding van opmerkingen gemaakt in de Eerste Kamer bij gelegenheid van de mondelinge behandeling van het wetsvoorstel computercriminaliteit (Handelingen I 1992/93, p. 11-452 e.v.). Inhoudelijke wijzigingen worden niet beoogd.

Het voorgestelde derde lid betreft de wijziging van de regeling van het onderzoek van gegevens in geautomatiseerde werken ten aanzien van voor raadpleging opgeslagen e-mail. Deze is in het algemeen deel reeds toegelicht. Over de gehanteerde terminologie merk ik nog het volgende op. "Gesloten elektronische berichten" dienen te worden onderscheiden van berichten op computernetwerken, bijv. Internet, die voor eenieder toegankelijk zijn. E-mails zijn gesloten, voor zover blijkt van de (geobjectiveerde) wil van betrokkene om het bericht vertrouwelijk te houden, blijkend uit enige beveiliging van het bericht, bijvoorbeeld door middel van een password. In dat geval valt de e-mail onder het recht op vertrouwelijke communicatie, zoals voorgesteld door voorstel 25 443 tot wijziging van de Grondwet, en gelden de hier voorgestelde extra eisen voor het onderzoek van e-mail. Voor het onderzoek van opgeslagen e-mail, die níet beveiligd is, gelden de algemene eisen van artikel 125i lid 1 en 2 Sv.

Met de woorden "opgeslagen ter *verdere* verzending" wordt uitgedrukt dat het gaat om e-mails die worden verstuurd door tussenkomst van een instelling van vervoer en niet om berichten die afkomstig zijn van zo'n instelling zelf en door deze gereed worden gehouden ter verzending naar anderen.

B

Dit betreft eveneens een taalkundige correctie. De woorden "voor zover" voegen niets toe.

C

Op grond van artikel 125k moet degene aan wie een zodanig bevel wordt gegeven, toegang verschaffen tot een geautomatiseerd werk door zijn kennis omtrent de beveiliging, of, ingeval de gegevens in het geautomatiseerd werk zijn versleuteld, de kennis omtrent de wijze van versleuteling ter beschikking te stellen. Deze kennis moet beschikbaar worden gesteld bij een huiszoeking (doorzoeking volgens wetsvoorstel 23 251) of bij toepassing van artikel 125j. In de praktijk komt het regelmatig voor dat bij een huiszoeking enkel de gegevens worden gekopieerd, waarna een nader onderzoek van die gegevens vervolgens op het politiebureau geschiedt. Ook in deze gevallen dient artikel 125k toepasselijk te zijn. Teneinde hierover alle misverstand te vermijden is dit artikel daarom gewijzigd in die zin dat het bevel als bedoeld kan worden gegeven "bij gelegenheid van een doorzoeking of de toepassing van artikel 125j".

D

Onderdeel D bevat een wijziging van artikel 125m in verband met de reeds bestaande medewerkingsplicht in geval van een huiszoeking (art. 125k Sv). In lijn met de voorgestelde wijziging van de artikelen 126m en 126t wordt erin voorzien dat het bevel tot medewerking aan de ontsleuteling onder omstandigheden ook kan worden gericht tot de verdachte. Het huidige derde lid

van artikel 125m Sv, betreffende de opgave aan de beheerder van een geautomatiseerd werk van de ten behoeve van de strafvordering vastgelegde gegevens, wordt, met enkele verruimingen, overgeheveld naar het nieuwe artikel 125p.

E

Artikel 125n Sv

De wijziging van de regeling van het onderzoek van e-mail is in het algemeen deel reeds toegelicht (zie ook onder A).

Artikel 125o

In het nieuwe artikel 125o Sv is de voorlopige maatregel van ontoegankelijkmaking van gegevens neergelegd. Deze is in het algemeen deel van de toelichting reeds toegelicht. Daaraan zij hier alleen toegevoegd dat de woorden "dan wel" in het eerste en derde lid aangeven dat lopende een gerechtelijk vooronderzoek de rechter-commissaris exclusief bevoegd is en de officier van justitie dus geen beslissingen over ontoegankelijkmaking mag nemen.

In dit wetsvoorstel worden, ten behoeve van de ontoegankelijkmaking en de vernietiging van gegevens, géén nieuwe zoekbevoegdheden voorgesteld. Beide maatregelen hebben slechts betrekking op gegevens die bij een onderzoek in een geautomatiseerd werk "worden aangetroffen". Dergelijk onderzoek moet op andere gronden berusten, zoals de mogelijkheid voor de RC om de "uitlevering" van computergegevens te bevelen (art. 125i Sv) of de huiszoekingsbevoegdheden. Ook is het mogelijk dat bij een zogenaamde netwerkzoeking - onderzoek vanaf de plaats van een huiszoeking in een elders aanwezig geautomatiseerd werk (art. 125j Sv) - in een computer elders strafbare gegevens worden aangetroffen. De hier voorgestelde bevoegdheid maakt het dan mogelijk die gegevens ontoegankelijk te maken. Ook is het mogelijk dat via Internet algemeen toegankelijke strafbare informatie wordt gevonden. Wanneer vaststaat dat het gaat om gegevens die onder Nederlandse rechtsmacht vallen, kan ook dan deze maatregel worden getroffen. In andere gevallen is de Nederlandse politie afhankelijk van het ingrijpen van de ter plaatse bevoegde rechterlijke autoriteiten.

Artikel 125p Sv

Op grond van de Aanbeveling nr. R (95) 13 van de Raad van Europa betreffende strafprocesrecht en informatietechnologie behoren belanghebbenden te worden geïnformeerd over vastlegging of ontoegankelijkmaking van computergegevens. Belanghebbend is allereerst de beheerder van het computersysteem, als degene die uit hoofde van zijn functie primair verantwoordelijk is voor het behoud en het gebruik van de gegevens die zijn opgeslagen in de aan zijn zorg toevertrouwde computers. Daarnaast kunnen anderen belanghebbend zijn (zie § 65 e.v. van het Explanatory memorandum). Het huidige artikel 125m, derde lid, Sv is in dit opzicht beperkter doordat het alleen een opgaveplicht schept ten aanzien van de beheerder. Voorgesteld wordt nu om in een nieuw artikel 125p een algemene opgaveplicht op te nemen, die zowel geldt bij de enkele vastlegging, tijdens een onderzoek in een geautomatiseerd werk, van computergegevens als bij de ontoegankelijkmaking van dergelijke gegevens, en die zowel verplicht tot mededeling aan de beheerder van de computer als tot mededeling aan belanghebbende derden. Verder is bepaald is dat de opgave aan de beheerder en andere belanghebbenden "zo spoedig mogelijk" dient te geschieden. Deze clausule strekt ter bescherming van het belangen die worden gediend door het privacyrecht, en laat geen uitstel van de opgave toe met het oog op het opsporingsbelang. Uitstel is slechts mogelijk onder de (hierna te bespreken) voorwaarden van het tweede lid.

Bij belanghebbenden anders dan de beheerder dient vooral te worden gedacht aan degenen die, met toestemming van de beheerder, toegang hebben tot de betrokken vastgelegde of ontoegankelijk gemaakte bestanden of de *directories* waarin die bestanden zich bevinden. (Voldoende) belanghebbend zijn deze personen evenwel slechts voor zover aannemelijk is dat zij deze bestanden hebben vervaardigd, bewerken of regelmatig raadplegen. Ook degene die onderwerp is van de (vermeend) strafbare uitingen, zoals degene wiens goede naam in een geschrift wordt geschaad (art. 261 Sr), zal als belanghebbende kunnen worden aangemerkt. Hij of zij heeft er immers een direct belang bij dat het strafbaar feit wordt beëindigd. Ook andere personen van wie gegevens voorkomen in bij een opsporingsonderzoek vastgelegde bestanden, kunnen onder omstandigheden als belanghebbenden worden aangemerkt, bijvoorbeeld vanwege het feit dat ze een zakelijke relatie onderhouden met een verdachte (leveranciers e.d.).

De opgave aan de beheerder en andere belanghebbenden bij gekopieerde gegevens stelt hen in staat om zich bij vermeende onrechtmatige uitoefening ten aanzien van hen van enige opsporingsbevoegdheid tot de rechter te wenden. Daartoe staat hun onder andere de weg van artikel 552a Sv open. Artikel 13 EVRM schrijft een dergelijke "effective remedy" voor. Geheime uitoefening van opsporingsmethoden die gericht zijn op het verzamelen van in het verleden opgeslagen informatie, is dus niet mogelijk. Hiertoe bestaat ook geen noodzaak aangezien de uitoefening van de bevoegdheid geen gevaar loopt door het bekend worden daarvan. Om deze reden kan evenmin van de beheerder worden verlangd dat hij de uitoefening van opsporingsbevoegdheden geheim houdt tegenover mogelijke derden-belanghebbenden. Een dergelijke geheimhouding heeft slechts zin wanneer de goede uitoefening van een opsporingsbevoegdheid in gevaar zou komen door het bekend worden daarvan bij de te onderzoeken subjecten, zoals bijvoorbeeld bij een telefoontap. In tegenstelling tot bijvoorbeeld een huiszoeking gaat het dan om een bevoegdheid die ertoe strekt informatie te vergaren gedurende een bepaalde tijd in de toekomst. De uitoefening van deze bevoegdheid zou van iedere betekenins zijn ontbloot wanneer degeen die wordt afgeluisterd, daarvan zou weten. De uitoefening van het grondrecht als verwoord in artikel 13 EVRM kan dan tijdelijk worden opgeschort, omdat zulks noodzakelijk is in verband met de goede uitvoering van deze bijzondere bevoegdheid. Het voorgestelde tweede lid van artikel 125p voorziet in een dergelijke opschorting voor het geval bij een opsporingsonderzoek vastgelegde computergegevens aanleiding zijn voor de uitoefening van een van de bevoegdheden zoals geregeld in wetsvoorstel 25 403 (bijzondere opsporingsbevoegdheden) ten aanzien van een bepaalde persoon. Vgl. de situatie dat een onderzoek in de elektronische zakagenda van een drugsdealer leidt tot het tappen van de in de agenda vermelde telefoonaansluitingen van zijn leveranciers. De opgave aan dergelijke belanghebbenden dat omtrent hen gegevens zijn vastgelegd, kan dan worden opgeschort zolang dit noodzakelijk is voor de uitoefening van de betrokken bevoegdheid ten aanzien van hen. Vanwege het uitzonderingskarakter van deze uitstelmogelijkheid is het oordeel hierover voorbehouden aan de officier van justitie dan wel, tijdens een gerechtelijk vooronderzoek, de rechter-commissaris.

De opgaveplicht ten aanzien van derde-belanghebbenden geldt slechts "voor zover dat (opgave van de gegevens) redelijkerwijs mogelijk is". Van de autoriteiten worden geen buitensporige inspanningen gevergd (zie § 69 van het Explanatory memorandum).

Voorts wordt de werkingssfeer van artikel 125p expliciet uitgebreid tot de inbeslagneming van voorwerpen waaraan computergegevens kunnen worden ontleend. Het is immers mogelijk dat een gegevensdrager in beslag wordt genomen en onderzocht buiten het kader van een huiszoeking of de toepassing van een van de bevoegdheden geregeld in de Zevende Afdeling van Titel IV van Boek I (vgl. artt. 96, 97, eerste lid, onderdeel 2, en 104, eerste lid, Sv). Over het algemeen wordt aangenomen dat de bevoegdheid tot inbeslagneming een bevoegdheid impliceert tot het verrichten van enig onderzoek aan het in beslag te nemen voorwerp. Dit onderzoek aan bijvoorbeeld een inbeslaggenomen, door de verdachte meegevoerde lap-top kan met zich brengen dat gegevens worden opgeslagen. Teneinde te bewerkstelligen dat ook in dergelijke gevallen een opgave aan de beheerder van het geautomatiseerd werk wordt gedaan van de gegevens die zijn vastgelegd, alsmede vernietiging van deze gegevens plaatsvindt zodra ze van geen betekenis meer zijn voor het

onderzoek (zie het voorgestelde art. 125q), wordt uitdrukkelijk in de artikelen 125p en 125q, eerste lid, bepaald dat ze ook toepasselijk zijn ingeval de toepassing van inbeslagneming tot vastlegging van gegevens heeft geleid.

F

Uitdrukkelijk wordt bepaald dat artikel 125q (125n oud) ook toepasselijk is ingeval de toepassing van inbeslagneming tot vastlegging van gegevens heeft geleid. Zie hiervoor de opmerking ten aanzien van art. 125p.

G en I

Deze onderdelen bevatten de in onderdeel E van het algemeen deel toegelichte aanpassing van de pseudokoopbepalingen zoals neergelegd in wetsvoorstel 25 403 (bijzondere opsporingsbevoegdheden) met het oog op het onderzoek op openbare computernetwerken.

H en J

Deze onderdelen bevatten de verplichting voor degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van gegevensverkeer dat onderwerp is van een tap, om mee te werken aan de ontsleuteling daarvan. Zie onderdeel C van het algemeen deel. Uitgegaan is van de tapbepalingen zoals die luiden na invoering van wetsvoorstel 25 403.

K

Het huidige artikel 353 Sv verzekert dat bij de einduitspraak steeds een beslissing wordt genomen over inbeslaggenomen voorwerpen. Het hier voorgestelde artikel 354 doet hetzelfde ten aanzien van ontoegankelijk gemaakte computergegevens. Als de rechter niet besluit tot vernietiging moet hij de gegevens weer ter beschikking van de beheerder doen stellen.

L

Zoals in par. 8 reeds aangegeven, wordt voorgesteld om de beklagmogelijkheid die reeds bestaat ten aanzien van de inbeslagneming van voorwerpen en bijvoorbeeld, sinds de eerste Wet computercriminaliteit, ten aanzien van de kennisneming of het gebruik van computergegevens vastgelegd tijdens een onderzoek in een geautomatiseerd werk, uit te breiden tot de ontoegankelijkmaking van strafbare gegevens op grond van artikel 125o Sv. Deze beklagmogelijkheid strekt primair tot bescherming van de rechten van degenen die, voordat de maatregel werd toegepast, toegang hadden tot de betrokken gegevensbestanden. Voor wie in dit verband als belanghebbenden kunnen worden aangemerkt, zie de toelichting op artikel 125p. De voorgestelde regeling biedt - naast het beklag over de ontoegankelijkmaking zelf - ook de mogelijkheid te klagen over het uitblijven van een last tot opheffing van de ontoegankelijkmaking en over de (voorgenomen) opheffing van de ontoegankelijkmaking. Dit laatste is met name van belang voor het slachtoffer dat er een direct belang bij heeft dat hij niet weer voorwerp wordt van een strafbaar feit.

Het is van belang dat, indien eenmaal een klaagschrift is ingediend, andere belanghebbenden dan de klager zoveel mogelijk bij de behandeling van dat klaagschrift worden betrokken. Artikel 552a, vierde lid, tweede volzin, bevat daarom een aanwijzing aan de voorzitter van het gerecht om andere belanghebbenden van het klaagschrift in kennis te doen stellen. Dit voorschrift behoort ook te gelden bij klaagschriften die betrekking hebben op vastgelegde of ontoegankelijk gemaakte

computergegevens. Dit wordt duidelijk gemaakt door de invoeging van de woorden "of dezelfde gegevens".

M

In het voorgestelde systeem van ontoegankelijkmaking en vernietiging van computergegevens is de definitieve beslissing voorbehouden aan de rechter. Dit betekent dat, net als bij de onttrekking aan het verkeer van voorwerpen, voorzien moet zijn in de mogelijkheid van vernietiging bij afzonderlijke rechterlijke beschikking voor het geval het niet tot een strafzaak komt. Hiertoe wordt artikel 552fa Sv voorgesteld, dat voor wat betreft de procedure aanknoopt bij artikel 552f Sv (over de onttrekking aan het verkeer).

Artikel III

Wat het overgangsrecht betreft gelden, op enkele uitzonderingen na, de hoofdregels, dat wil zeggen ten aanzien van de wijzigingen in de strafbepalingen artikel 1 Sr en ten aanzien van de strafvorderlijke bepalingen het beginsel van onmiddellijke werking. Ook de wijzigingen van de artikelen 53 en 54 Sr hebben onmiddellijke werking. Dit betekent dat tussenpersonen die na inwerkingtreding van de wet voldoen aan de nieuwe voorwaarden niet kunnen worden vervolgd wegens (medeplichtigheid aan) een uitings- of verspreidingsdelict gepleegd voor die inwerkingtreding.

Voor een aantal situaties is een bijzondere overgangsregeling getroffen. Onderdeel 1 van dit artikel stelt zeker dat gesloten elektronische berichten (e-mails) die voorafgaand aan inwerkingtreding van deze wet door een rechter-commissaris, een officier van justitie of een opsporingsambtenaar zijn vergaard, mogen worden geopend en ingezien óók als ze niet onder de restrictieve(re) voorwaarden van het nieuwe artikel 125n zouden vallen. Vóór inwerkingtreding van dit artikel kende de wet immers geen andere restricties voor de inzage in computergegevens dan die onder andere gelegen in het oude artikel 125i Sv.

Onderdeel 2 ziet op het geval waarin het wetsvoorstel voorziet in de mogelijkheid om een bevel op grond van art. 125k Sv (medewerking aan de ontsleuteling ter gelegenheid van een huiszoeking) aan de verdachte te geven en op het geval waarin aan bepaalde personen (waaronder de verdachte) de verplichting kan worden opgelegd mee te werken aan het ontsleutelen van gegevensverkeer dat is afgetapt (art. 126m lid 5 Sv en 126t lid 5 Sv). Deze bevelen zijn gekoppeld aan de uitoefening van een andere bevoegdheid - de bevoegdheid tot het doorzoeken van plaatsen en de tapbevoegdheid - en kunnen in zoverre als accessoire bevoegdheden worden beschouwd. Gelet hierop brengt de rechtszekerheid mijns inziens mee dat, wanneer de hoofdbevoegdheid is uitgeoefend vóór inwerkingtreding van deze wet - op welk moment de (accessoire) medewerkingsverplichtingen nog niet bestonden -, de betrokkene niet daarná alsnog tot medewerking aan de ontsleuteling van de verkregen gegevens kan worden gedwongen.

Onderdeel 3 ziet op de bevoegdheid tot "pseudokoop" van computergegevens door tussenkomst van een openbaar telecommunicatienetwerk en voorziet in de mogelijkheid om als het ware vooruit te lopen op de nieuwe regeling. Een dergelijke mogelijkheid is ook opgenomen in het wetsvoorstel bijzondere opsporingsbevoegdheden. Een bevel dat materieel voldoet aan de voorwaarden gesteld in de artikelen 126i en 126q Sv, geldt vanaf inwerkingtreding van deze wet als een bevel in de zin van die artikelen.

De Minister van Justitie,