Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met ontoegankelijkmaking van gegevens op het internet, strafbaarstelling van het wederrechtelijk overnemen van gegevens en het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens, alsmede verruiming van de strafbepalingen betreffende het afluisteren, aftappen of opnemen van vertrouwelijke communicatie (versterking bestrijding computercriminaliteit)

MEMORIE VAN TOELICHTING

I. ALGEMEEN

1. Inleiding

In dit wetsvoorstel wordt voorgesteld om met het oog op versterking van de bestrijding van computercriminaliteit een drietal wetswijzigingen door te voeren. In de eerste plaats wordt voorgesteld te komen tot een zelfstandige regeling van de bevoegdheid van de officier van justitie te vorderen gegevens op het internet ontoegankelijk te maken. De bedoeling is de strafrechtelijke mogelijkheden om "strafbare content" effectief en doelmatig van het internet te verwijderen, verder te versterken, vooral in gevallen waarin internetproviders daartoe niet op basis van vrijwilligheid overgaan.

In de tweede plaats wordt in dit wetsvoorstel voorgesteld het wederrechtelijk overnemen van computergegevens en het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens strafbaar te stellen. Hiermee wordt een betere strafrechtelijke bescherming geboden tegen het wederrechtelijk overnemen van computergegevens. Dat kan aan de hand van enkele voorbeelden worden geïllustreerd. Zo wordt de persoon strafbaar die rechtmatige toegang heeft tot in een computer opgeslagen persoonlijke gegevens betreffende een bekende Nederlander, en die deze gegevens kopieert. Voorts worden personen strafbaar die uit de computer van anderen ontvreemde gegevens tot hun beschikking hebben en/of op het internet plaatsen, zoals het geval was bij de digitale naaktfoto's van een bekende presentatrice. Hiermee zal ook degene die zich erop beroept deze gegevens niet zelf te hebben ontvreemd, maar van een derde te hebben verkregen, strafbaar zijn. Daardoor worden ook gedragingen strafbaar die kunnen worden beschouwd als "heling" van computergegevens.

In de derde en laatste plaats verruimt het wetsvoorstel de strafbepalingen betreffende het afluisteren, aftappen of opnemen van vertrouwelijke communicatie. Thans zijn personen die stiekem – zonder dat de andere gespreksdeelnemer(s) daarvan

weet/weten – vertrouwelijke communicatie opnemen alleen strafbaar als het gaat om communicatie tussen anderen. Door de voorgestelde verruiming worden ook personen strafbaar die stiekem communicatie opnemen waaraan zij zelf deelnemen en/of de desbetreffende gegevens vervolgens over het internet verspreiden.

De voortschrijdende ontwikkelingen op het terrein van de informatie- en communicatietechnologie, waardoor het overnemen van computergegevens en het breed over het internet verspreiden daarvan steeds eenvoudig worden, maken het noodzakelijk om ter bescherming van de persoonlijke levenssfeer van de burgers en van vertrouwelijke communicatie, computergegevens een ruimere strafrechtelijke bescherming te bieden. Dit wetsvoorstel voorziet daarin.

De snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit roepen voortdurend de vraag op of de juridische instrumenten nog voldoende zijn toegesneden om computercriminaliteit effectief te bestrijden. Deze vraag is niet nieuw. Reeds aan het begin van de jaren negentig van de vorige eeuw was de vraag aan de orde in hoeverre het materiële strafrecht in alle opzichten voldoende bescherming biedt tegen de mogelijkheden om met nieuwe informatietechnieken gerechtvaardigde belangen te schaden. Met de Wet computercriminaliteit, in werking getreden op 1 maart 1993, is het Wetboek van Strafvordering aangevuld met bevoegdheden op het gebied van het onderzoek van geautomatiseerde werken en zijn specifieke strafbepalingen rond de wederrechtelijke toegang tot computers en het misbruik van gegevens toegevoegd aan het Wetboek van Strafrecht. Met de Wet computercriminaliteit II, in werking getreden op 1 september 2006, is hieraan een vervolg gegeven en zijn het Wetboek van Strafrecht en het Wetboek van Strafvordering aangepast aan de nieuwe ontwikkelingen in de informatietechnologie. Aanleiding daarvoor vormde de beleidsnota "Wetgeving voor de elektronische snelweg" (Kamerstukken II 1997/98, 25 880, nrs. 1-2), alsmede in een later stadium, het te Boedapest tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290), ook bekend als het Cybercrimeverdrag.

In 2008 is aan de Tweede Kamer een beleidskader voor de rechtshandhaving bij cybercrime in het algemeen en internetmisbruik in het bijzonder aangeboden (Kamerstukken II 2007/08, 28 684, nr. 133). Zoals daarin werd aangekondigd zijn de knelpunten in het juridisch instrumentarium voor de bestrijding van cybercrime in samenspraak met de betrokken partijen geïnventariseerd. Bij brief van 26 juni 2009 is de Tweede Kamer een, op basis van deze inventarisatie verrichte, verkenning naar de toereikendheid van de relevante juridische instrumenten toegezonden (Kamerstukken II 2008/09, 28 684, nr. 232). De belangrijkste conclusie van deze verkenning is dat er grote behoefte bestaat aan uitleg over

de wet– en regelgeving en over de toepassing van (bijzondere) opsporingsbevoegdheden op het internet. Daarnaast is in deze brief aangegeven dat de verkenning aanleiding geeft tot enkele aanpassingen van de wetgeving. Deze aanpassingen, die hierboven zijn beschreven, worden in het navolgende nader toegelicht. In paragraaf 2 komt de voorgestelde zelfstandige bevoegdheid van de officier van justitie te vorderen dat gegevens ontoegankelijk worden gemaakt, aan de orde. Paragraaf 3 is gewijd aan strafbaarstelling van het wederrechtelijk overnemen van gegevens en het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens. Paragraaf 4 betreft verruiming van de strafbepalingen betreffende het afluisteren, aftappen of opnemen van vertrouwelijke communicatie. Ten slotte volgt de artikelsgewijze toelichting. Zoals in de brief van 29 juni 2009 aan de Tweede Kamer is aangegeven, wordt thans nader de behoefte onderzocht aan een regeling aangaande het online doorzoeken. Om deze reden wordt dit onderwerp niet in dit wetsvoorstel geadresseerd.

Over het concept van dit wetsvoorstel zijn adviezen ontvangen van ..
PM

2. De vordering tot het ontoegankelijk maken van gegevens

Voorgesteld wordt de bevoegdheid van de officier van justitie te vorderen dat gegevens ontoegankelijk worden gemaakt als afzonderlijke en zelfstandige bevoegdheid op te nemen in (de artikelen 125p en 125q van) het Wetboek van Strafvordering (Sv). De bevoegdheid is van belang in die gevallen waarin de aanbieder van een communicatiedienst of degene die de beschikkingsmacht heeft over een geautomatiseerd werk, niet bereid is op basis van de gedragscode "Notice and Take Down" de gegevens ontoegankelijk te maken en de vordering nodig is om het strafbare feit te beëindigen of om nieuwe strafbare feiten te voorkomen. Voorgesteld wordt de officier van justitie de bevoegdheid te verlenen in de vordering zo nodig een dwangsom op te leggen voor het geval niet aan de vordering wordt voldaan.

Het is uit wetssystematisch oogpunt gewenst dat de bevoegdheid om de ontoegankelijkmaking van gegevens te vorderen in het Wetboek van Strafvordering wordt opgenomen in plaats van – zoals thans het geval is – in (artikel 54a van) het Wetboek van Strafrecht (Sr). Artikel 54a Sr bevat, naast een bevoegdheid van de officier van justitie om ontoegankelijkmaking van gegevens te bevelen, ook een – onder nadere voorwaarden toepasselijke – vervolgingsuitsluitingsgrond voor aanbieders van een communicatiedienst. Deze vervolgingsuitsluitingsgrond is in het Wetboek van Strafrecht opgenomen ter uitvoering van de Richtlijn inzake elektronische handel, die er onder andere toe strekt de aansprakelijkheid van intermediaire dienstverleners van de informatiemaatschappij te

beperken. Uit de rechtspraak met betrekking tot artikel 54a Sr kan worden afgeleid dat onder andere de combinatie van een vervolgingsuitsluitingsgrond en een bevelsbevoegdheid in één bepaling vragen oproept en de toepassing van de regeling in de praktijk compliceert (zie Rechtbank Assen 22 juli 2008, LJN BD8451, Hof Leeuwarden 20 april 2009, LJN BI1645 en Rechtbank Assen 24 november 2009, LJN BK4226). Opneming van de bevoegdheid de ontoegankelijkmaking van gegevens te vorderen in het Wetboek van Strafvordering is daarmee niet alleen uit wetssystematisch oogpunt, maar ook uit een oogpunt van overzichtelijkheid en duidelijkheid voor de praktijk van belang. Van de gelegenheid is gebruik gemaakt om de vervolgingsuitsluitingsgrond die in artikel 54a Sr resteert op enkele punten te verhelderen en meer toe te snijden op de gedragscode "Notice and Take Down". De daartoe strekkende bijstellingen worden artikelsgewijs toegelicht.

De hoofdlijnen van de regeling, die wordt neergelegd in de voorgestelde artikelen 125p en 125q Sv, zijn de volgende. Zoals gezegd is de voorgestelde regeling, evenals de bestaande regeling van artikel 54a Sr, bedoeld voor de gevallen waarin de zelfregulering binnen de bedrijfstak tekort schiet. Zoals in de, hierboven in paragraaf 1 genoemde, brief aan de Tweede Kamer is gemeld (Kamerstukken II 2008/09, 28 684, nr. 232), is er inmiddels op basis van vrijwilligheid een gedragscode opgesteld en ondertekend door een groot aantal internetproviders. Dit betreft de gedragscode "Notice and Take Down" (verder: NTD-gedragscode). De NTD-gedragscode richt zich op tussenpersonen die in Nederland een openbare telecommunicatiedienst op het internet leveren en bevat een procedure voor het omgaan met meldingen van onrechtmatige en strafbare informatie op het internet. Indien er naar het oordeel van de tussenpersoon sprake is van onmiskenbaar onrechtmatige of strafbare inhoud, zorgt de tussenpersoon ervoor dat de betreffende inhoud onverwijld verwijderd wordt. Indien niet tot een eenduidig oordeel wordt gekomen of er al dan niet sprake is van onrechtmatige of strafbare inhoud, kan de melder overgaan tot het doen van aangifte of de rechter betrekken. Deze procedure wordt eveneens toegepast bij verzoeken van de politie als het gaat om het verwijderen van afbeeldingen van kinderporno van het internet die in Nederland wordt "gehost". In die gevallen waarin de NTD-gedragscode niet afdoende is voor de verwijdering van de gegevens, kan de officier van justitie gebruik maken van de bevoegdheid van het voorgestelde artikel 125p Sv.

Om de vordering, in gevallen waarin daartoe aanleiding is, kracht bij te kunnen zetten is in het voorgestelde artikel 125q Sv voorzien in de mogelijkheid zo nodig een dwangsom op te leggen voor gevallen waarin niet aan de vordering wordt voldaan. Dat is als "stok achter de deur" in geval snelle ontoegankelijkmaking van gegevens ter voorkoming of beïndiging van strafbare feiten noodzakelijk is, effectiever dan het instellen van strafvervolging voor het niet voldoen aan de vordering, hetgeen mogelijk is op grond van artikel 184 Sr waarin het

niet voldoen aan een bevoegd gegeven ambtelijk bevel strafbaar is gesteld. Voor de – artikelsgewijs verder toegelichte – uitwerking van de dwangsom wordt aansluiting gezocht bij de Algemene wet bestuursrecht.

Evenals het geval is onder de bestaande regeling van artikel 54a Sr kan ingevolge de in het voorgestelde artikel 125p Sv opgenomen regeling alleen ontoegankelijkmaking van de gegevens worden gevorderd. Over de vraag of deze gegevens vervolgens moeten worden vernietigd, beslist de rechter. Belanghebbenden kunnen zich bij de raadkamer van de rechtbank schriftelijk beklagen over de vordering tot het ontoegankelijk maken van gegevens op grond van de bestaande beklagregeling voor inbeslaggenomen voorwerpen (artikel 552a Sv). Indien in de vordering een dwangsom is opgelegd, kan het beklag zich daartoe mede uitstrekken. Mede door introductie van de mogelijkheid zich bij de raadkamer van de rechtbank over de vordering te beklagen, is handhaving van de in het huidige artikel 54a Sr opgenomen voorwaarde van een voorafgaande schriftelijke machtiging door de rechter-commissaris, niet meer noodzakelijk.

3. Het wederrechtelijk overnemen van gegevens en het beschikken over en bekend maken van wederrechtelijk overgenomen gegevens

Een tweede element van dit wetsvoorstel betreft strafbaarstelling van het wederrechtelijk overnemen van gegevens uit bijvoorbeeld een computer en strafbaarstelling van het beschikken over of bekend maken van gegevens die wederrechtelijk zijn overgenomen. Met de eerstgenoemde strafbaarstelling – wederrechtelijk overnemen van gegevens – wordt een betere bescherming geboden tegen het overnemen van gegevens uit computers, in die gevallen waarin de gegevens gekopieerd zijn en de rechthebbende dus de beschikking houdt over de gegevens. De rechthebbende heeft echter geen invloed op het gebruik dat vervolgens van de overgenomen gegevens wordt gemaakt, waardoor hij benadeeld kan worden. Met de als tweede genoemde strafbaarstelling wordt strafrechtelijke aansprakelijkheid geschapen van degene die over dergelijke gegevens beschikt of deze bekend maakt. Langs deze weg wordt “heling” van de desbetreffende gegevens strafbaar gesteld. Strafbaarstelling van het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens is ook van belang in situaties waarin niet aangetoond kan worden dat de persoon die deze gegevens bekend maakt degene is die deze gegevens zelf heeft overgenomen, al dan niet na in een geautomatiseerd werk te zijn binnengedrongen, bijvoorbeeld door het “hacken” van een computer. Hierboven in paragraaf 1 zijn enkele voorbeelden gegeven van gedragingen die door het hier besproken element van het wetsvoorstel strafbaar worden.

Met het voortschrijden van de informatie- en communicatietechnologie neemt het maatschappelijke belang van gegevens steeds verder toe. De technische ontwikkelingen nopen tot een verdere strafrechtelijke bescherming van gegevens. Door deze ontwikkelingen wordt het steeds eenvoudiger om gegevens uit een computer over te nemen en vervolgens op het internet te zetten. Daardoor kan het gebeuren dat vertrouwelijke gegevens razend snel worden verspreid en voor grote groepen mensen toegankelijk worden. Het is bovendien niet eenvoudig om over het internet verspreide gegevens daarvan geheel verwijderd te krijgen. Het uit een computer overnemen van gegevens over personen, en die gegevens vervolgens op het internet zetten zijn verwerpelijke gedragingen waartegen adequaat strafrechtelijk moet kunnen worden opgetreden, vooral met het oog op bescherming van de persoonlijke levenssfeer van degene wiens gegevens het betreft. De personen die zich aan dergelijke handelingen schuldig maken kunnen weten dat het hier om verwerpelijke gedragingen gaat.

Uit het hierboven in paragraaf 1 genoemde onderzoek is gebleken dat de strafrechtelijke bescherming van gegevens verbetering behoeft. Het door middel van het internet ("op afstand") binnendringen in een computer is technisch zeer goed mogelijk. Het doel van een dergelijke activiteit kan zijn om gevoelige gegevens te achterhalen, zoals bankrekeningnummers of wachtwoorden. Ook kan het gaan om het overnemen van gegevens uit een emailbox. Gebleken is dat het niet mogelijk is een persoon te vervolgen voor "heling" van gegevens die door middel van computervredebreuk uit een computer zijn gekopieerd. Het College van procureurs-generaal heeft – bij gelegenheid van de consultatie over het ontwerp van het aan de Wet van 12 juni 2009, Stb. 245 ten grondslag liggende wetsvoorstel – aandacht gevraagd voor de onmogelijkheid iemand te vervolgen voor het "helen" van dergelijke gegevens (Kamerstukken II 2007/08, 31 386, nr. 3, blz. 2). Bij verschillende gelegenheden is gebleken dat behoefte bestaat aan een dergelijke mogelijkheid. Dit betrof volgens het College onder meer een geval waarbij gegevens door computervredebreuk uit een emailbox waren gekopieerd, en vervolgens aan een derde doorgegeven. Deze derde heeft de gegevens, ondanks dat vrijwel vaststond dat hij moest weten dat zij door misdrijf waren verkregen, in ontvangst genomen en door middel van het internet gepubliceerd. Omdat het in deze zaak om (gekopieerde) gegevens ging, en niet om een goed, kon deze derde niet strafrechtelijk aansprakelijk worden gesteld voor heling van een goed. De hacker van de gegevens kon worden vervolgd wegens computervredebreuk (artikel 138a Sr). Inmiddels hebben ook andere gevallen in de media de nodige aandacht gekregen, zoals de publicatie op het internet van door computervredebreuk verkregen digitale naaktfoto's van een bekende presentatrice. Naar aanleiding van dit geval zijn Kamervragen gesteld over de noodzaak om "heling" van gegevens strafbaar te stellen. Bij de beantwoording van die vragen heb ik aangegeven dat strafbaarstelling van heling van

gegevens bij het onderzoek van de knelpunten in het juridisch instrumentarium zal worden betrokken en dat de mogelijkheden voor een juridische vormgeving van een dergelijke strafbaarstelling zullen worden onderzocht (Handelingen II 2007/08, nr. 888). Dit onderdeel van het voorliggende wetsvoorstel vormt het resultaat daarvan.

Computercriminaliteit en gegevens zijn onlosmakelijk met elkaar verbonden. In veel gevallen is computercriminaliteit gericht op het wederrechtelijk vergaren van gegevens en het vervolgens gebruiken van deze gegevens bij het begaan van andere misdrijven. Het inbreken in computers van bedrijven om gegevens over creditcards te achterhalen of het door middel van het zogenaamde "phishen" (het opzetten van een valse website) ontfutselen van bancaire gegevens en pincodes zijn hier inmiddels bekende voorbeelden van. Phishing (of: identity theft) is strafbaar als een vorm van oplichting (artikel 326 Sr). Vereist is – kort gezegd – dat een persoon door middel van misleiding wordt gebracht tot de afgifte van een goed of van gegevens. Niet (meer) vereist is dat deze gegevens een geldswaarde in het handelsverkeer hebben.

Burgers, bedrijven en de overheid zijn zich in toenemende mate bewust van de gevaren die aan het misbruik van gegevens verbonden zijn en investeren het nodige om hun gegevens tegen onrechtmatige toegang en gebruik te beschermen. Gelet op de maatschappelijke belangen die op het spel staan bij het onrechtmatige bezit of gebruik van gegevens is het echter van belang dat de strafrechtelijke bescherming van gegevens verder wordt verstrekt.

Met de Wet computercriminaliteit is er destijds voor gekozen om gegevens begripsmatig afzonderlijk te behandelen en niet gelijk te stellen aan een "goed" (Kamerstukken II 1989/90, 21 551, nr. 3, blz. 3). Ook in de jurisprudentie van de Hoge Raad is de gelijkstelling van gegevens aan een goed afgewezen (HR 3 december 1996, NJ 1997, 574). Doorslaggevend argument is dat een "goed" individualiseerbaar is en dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft. Gegevens kunnen daarentegen worden overgenomen zonder dat de rechthebbende de beschikkingsmacht over de gegevens verliest. De rechthebbende kan echter geen invloed uitoefenen op het gebruik dat vervolgens van de overgenomen gegevens wordt gemaakt, waardoor hij benadeeld kan worden als de gegevens worden geopenbaard of anderszins worden aangewend op een wijze waardoor zijn belangen worden geschaad. Daar waar de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht is strafvervolging op grond van diefstal volgens enkele uitspraken van feitenrechters niet uitgesloten. Een voorbeeld hiervan betreft de diefstal van een virtueel amulet en een virtueel masker uit een online computerspel (Hof Leeuwarden 10 november 2009, LJN BK2773).

Het onderscheid dat met de Wet computercriminaliteit is gemaakt tussen het begrip goed en het begrip gegevens, heeft ertoe geleid dat in het Wetboek van Strafrecht en het Wetboek van Strafvordering specifieke bepalingen zijn opgenomen met betrekking tot gegevens. Zo kent het Wetboek van Strafrecht afzonderlijke strafbaarstellingen van computervredebreuk (artikel 138a Sr), het wederrechtelijk aftappen of opnemen van gegevens (artikel 139c Sr), het beschikken over of bekend maken van gegevens die zijn afgetapt, opgenomen of afgeluisterd (artikel 139e Sr), het "vernielen" van gegevens (artikelen 350a en 350b Sr), het bekendmaken of uit winstbejag gebruiken van gegevens over een onderneming (artikel 273 Sr), alsmede een strafbaarstelling van de persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of -dienst en die wederrechtelijk niet voor hem bestemde gegevens overneemt (artikel 273d Sr). Op grond van het meervoudige karakter van gegevens is bij de Wet computercriminaliteit bewust afgezien van specifieke bepalingen met betrekking tot inbeslagneming, onttrekking aan het verkeer en verbeurdverklaring van gegevens.

In lijn met de keuze die destijds bij de Wet computercriminaliteit en de Wet computercriminaliteit II is gemaakt, is ervoor gekozen de benodigde verbeteringen in de strafrechtelijke bescherming van gegevens door te voeren in de strafbepalingen die bij die wetten in de Vijfde Titel van het Tweede Boek van het Wetboek van Strafrecht zijn opgenomen. Het – in het algemeen – strafbaar stellen van het wederrechtelijk overnemen van gegevens die zijn opgeslagen door middel van een geautomatiseerd werk sluit aan bij de in die titel opgenomen strafbaarstelling van het wederrechtelijk aftappen en opnemen van dergelijke gegevens (artikel 139c Sr). Bovendien is het overnemen van gegevens uit een geautomatiseerd werk door iemand die daarin wederrechtelijk is binnengedrongen ook reeds in die titel strafbaar gesteld (artikel 138a Sr). Het wederrechtelijk overnemen van gegevens is voorts, zoals hierboven al kort werd aangestipt, strafbaar gesteld voor zover dit gebeurt door een persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of –dienst (artikel 273d Sr). De door het voortschrijden van de informatie- en communicatietechnologie wenselijke versterking van de strafrechtelijke bescherming van gegevens brengt mee dat het wederrechtelijk overnemen van gegevens in het algemeen strafbaar wordt gesteld.

Voor strafbaarheid van het wederrechtelijk overnemen van gegevens is niet – zoals in artikel 138a, tweede lid, Sr – vereist dat het geautomatiseerde werk waaruit de gegevens worden overgenomen, is binnengedrongen. Met andere woorden: de gegevens behoeven niet door computervredebreuk te zijn verkregen. De voorgestelde strafbaarstelling is, in aanvulling op de strafbaarstelling van computervredebreuk, vooral van belang voor gevallen

waarin de dader rechtmatige toegang heeft tot niet openbare gegevens van een computer, en deze gegevens wederrechtelijk overneemt. Daarbij kan worden gedacht aan de werknemer die gegevens waartoe hij uit hoofde van zijn functie toegang heeft, kopieert met de bedoeling deze voor zichzelf of voor een ander te gebruiken. Om deze reden stel ik voor artikel 139c Sr zo te wijzigen dat niet alleen het aftappen of opnemen van gegevens maar ook het overnemen van gegevens – in het algemeen – strafbaar wordt. Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen. Er is dan als het ware sprake van "verduistering" van gegevens, met dien verstande dat de rechthebbende de beschikkingsmacht over de gegevens behoudt, in welk geval strafvervolging op grond van artikel 321 Sr niet mogelijk is. Met het gebruik van de term "overnemen" wordt tot uitdrukking gebracht dat niet is vereist dat de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht. Het opzettelijk en wederrechtelijk overnemen van de gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, vormt daarmee een zelfstandige strafbare gedraging.

Verder acht ik het wenselijk de gedraging strafbaar te stellen die kan worden omschreven als het "helen" van de hier besproken gegevens. Met de voorgestelde wijziging van artikel 139e Sr wordt de persoon die de beschikking heeft over wederrechtelijk overgenomen gegevens of die dergelijke gegevens opzettelijk ter beschikking stelt aan een ander of aan een ander bekend maakt, voortaan strafbaar. Hiermee wordt een voorziening getroffen voor niet alleen de gevallen waarin iemand gegevens beschikbaar heeft die eerder door een ander wederrechtelijk zijn overgenomen, maar ook voor gevallen waarin niet kan worden bewezen dat degene die de beschikking heeft over de gegevens deze heeft verkregen doordat hij deze zelf wederrechtelijk heeft overgenomen, al dan niet door middel van computervredebreuk. Het is daarbij niet per se noodzakelijk dat de dader weet dat de gegevens door wederrechtelijk overnemen (aftappen, opnemen of afluisteren) zijn verkregen; voldoende is dat hij redelijkerwijs moet vermoeden dat zulks het geval is.

Samenvattend: met de voorgestelde aanpassing van de artikelen 139c en 139e Sr wordt de rechthebbende van gegevens een betere bescherming geboden tegen personen die de gegevens waar zij rechtmatig toegang toe hebben kopiëren, zonder dat er sprake is van computervredebreuk. Tevens wordt voorzien in een strafbaarstelling van een gedraging die zou kunnen worden aangemerkt als "heling" van dergelijke gegevens.

Het beschikken over of bekend maken van gegevens die door wederrechtelijk afluisteren, aftappen of opnemen zijn verkregen, wordt thans strafbaar gesteld met gevangenisstraf van

zes maanden of geldboete van de vierde categorie (artikel 139e Sr). Gelet op de ernst van de gedraging wordt voorgesteld de maximale gevangenisstraf te verhogen tot een jaar. Met de voorgestelde verhoging wordt de maximale gevangenisstraf gelijk aan die van het wederrechtelijk aftappen of opnemen van gegevens die via telecommunicatie of een geautomatiseerd werk worden verwerkt of overgedragen (artikel 139c Sr). In vergelijking met de strafbepalingen betreffende heling van een goed is het verhoogde strafmaximum voor het bezitten of bekendmaken van de hierboven genoemde gegevens in evenwicht; op schuldheling is een maximale gevangenisstraf gesteld van een jaar (artikel 417bis Sr) en op opzetheling vier jaar (artikel 416 Sr). Daarbij kan worden aangetekend dat in geval de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, volgens de hierboven bedoelde uitspraken van enkele feitenrechters kan worden aangenomen dat van diefstal van een goed sprake is; in die lijn ligt dat de helingsbepalingen van toepassing kunnen zijn op gegevens waarover de rechthebbende de beschikkingsmacht heeft verloren. In geval van opzettelijk handelen is in dat geval bij deze gegevens het strafmaximum van vier jaar beschikbaar.

Overwogen is het wederrechtelijk overnemen van gegevens, alsmede het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens, strafbaar te stellen als diefstal, verduistering en heling (artikelen 310, 321, 416 en 417bis Sr). Nadeel daarvan zou zijn dat zou worden afgeweken van de keuze uit de Wet computercriminaliteit en de Wet computercriminaliteit II om gegevens niet aan een goed gelijk te stellen. Diefstal of verduistering van gegevens strafbaar stellen is een minder geschikte oplossing in geval de gegevens zijn gekopieerd en de rechthebbende de beschikkingsmacht daarover dus niet heeft verloren. En indien de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, is volgens de hierboven bedoelde uitspraken van enkele feitenrechters sprake van diefstal van een goed, en valt dit gedrag (ook) onder artikel 310 Sr in zijn huidige vorm. Voorts zou een gelijkstelling van gegevens met goederen in de artikelen betreffende diefstal, verduistering en heling leiden tot een aanzienlijke overlap met de verschillende andere (al bestaande) artikelen betreffende gegevens (namelijk: de artikelen 139c, 139e, 273 en 273d).

4. Verruiming van de strafbaarstellingen betreffende afluisteren, aftappen of opnemen van vertrouwelijke communicatie

Het derde element van dit wetsvoorstel betreft verruiming van de strafbaarstellingen van het met een technisch hulpmiddel afluisteren, aftappen of opnemen van vertrouwelijke communicatie, en wel door de voorwaarde dat de dader geen gespreksdeelnemer is, alsmede de voorwaarde dat de gegevens niet bestemd zijn voor degene die deze gegevens

aftapt of opneemt, te laten vervallen. Ook dit voorstel is, naar hierboven in paragraaf 1 aan de orde kwam, ingegeven door de voortschrijdende technische ontwikkelingen die het betrekkelijk eenvoudig maken om gegevens af te tappen of op te nemen en op ruime schaal te verspreiden.

Het afluisteren of opnemen van gesprekken en het aftappen of opnemen van gegevens die door middel van telecommunicatie of een geautomatiseerd werk worden overgedragen is in het Wetboek van Strafrecht strafbaar gesteld. Daarbij wordt onderscheid gemaakt tussen het met een technisch hulpmiddel afluisteren of opnemen van een gesprek dat wordt gevoerd in een woning, besloten lokaal of erf (artikel 139a Sr), het afluisteren of opnemen van een gesprek dat elders wordt gevoerd (artikel 139b Sr) en het aftappen of opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of een geautomatiseerd werk (artikel 139c Sr). In alle gevallen geldt de voorwaarde dat de dader geen gespreksdeelnemer is dan wel dat de gegevens niet bestemd zijn voor degene die de gegevens aftapt of opneemt. De strafbaarstellingen betreffen dus communicatie tussen andere personen. Destijds werd door de wetgever geoordeeld dat het opnemen van gesprekken door een gespreksdeelnemer weliswaar onethisch kan zijn, of onrechtmatig kan zijn jegens de andere gespreksdeelnemer(s), maar dat het minder passend was dit strafbaar te stellen (Kamerstukken II 1967/68, 9419, nr. 3, blz. 5). Door de genoemde technische ontwikkelingen moet dit, om redenen die hieronder nog nader worden aangeduid, thans anders beoordeeld worden.

De voorgestelde wijziging sluit aan bij een recente wijziging van de bestaande wetgeving. Met de inwerkingtreding van de Wet van 8 mei 2003 tot wijziging van de artikelen 139f en 441b van het Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht) (Stb. 365), is met ingang van 1 januari 2004 het heimelijk met gebruikmaking van een technisch hulpmiddel vervaardigen van een afbeelding van een persoon die zich in een woning of op een andere niet voor het publiek toegankelijke plaats bevindt, strafbaar gesteld (artikel 139f Sr). Voor strafbaarheid is voldoende dat het opnemen van het beeldmateriaal heimelijk geschiedt. Niet noodzakelijk is dat dader zelf niet interacteert met de persoon van wie hij heimelijk een afbeelding vervaardigt.

Inmiddels zijn de technische ontwikkelingen zodanig voortgeschreden dat het betrekkelijk eenvoudig is om heimelijk gesprekken of andere vormen van communicatie op te nemen en vervolgens door middel van het internet breed te verspreiden. Dergelijke handelingen kunnen ingrijpende gevolgen hebben voor de slachtoffers. Hun persoonlijke levenssfeer wordt geschonden doordat gegevens, ten aanzien waarvan zij in de veronderstelling verkeren dat die uitsluitend bij henzelf en bij degene(n) bekend zijn met wie de communicatie is gevoerd, kunnen worden vastgelegd en verspreid. De kring van personen

die vervolgens van de inhoud van deze gegevens kennis kunnen nemen is vrijwel onbegrensd. Daar komt bij, dat het verwijderen van deze gegevens, als deze op het internet zijn geplaatst, in de praktijk niet altijd eenvoudig is. Het is dan ook wenselijk om de strafbaarstellingen van het afluisteren en opnemen van gesprekken en het aftappen en opnemen van gegevens die door telecommunicatie of een geautomatiseerd werk worden verwerkt, te verruimen zodat voortaan (onder overigens gelijkblijvende voorwaarden) ook strafbaar is het opnemen van gesprekken en communicatie waaraan de dader zelf deelneemt.

Aan de bestaande strafbaarstellingen die hierboven zijn genoemd ligt ten grondslag dat communicatie ten aanzien waarvan de gerechtvaardigde verwachting mag worden gekoesterd dat deze vertrouwelijk is, strafrechtelijke bescherming verdient. Dit achterliggende belang verdient ook strafrechtelijke bescherming als daarop een inbreuk wordt gemaakt door iemand die aan de communicatie deelneemt. Gewezen kan worden op het recht van Duitsland en Frankrijk waarin strafbaar is gesteld het opnemen van vertrouwelijk gesproken woorden van een ander, alsmede het ter beschikking stellen en openbaar maken van een dergelijke opname aan een ander (artikel 201 Strafgesetzbuch respectievelijk artikelen 226-1 en 226-2 Code Pénal). Een en ander is in die rechtstelsels ook strafbaar in geval sprake is van een gesprek waaraan degene die het opneemt zelf deelneemt. Dit onderdeel van het wetsvoorstel is daarmee in lijn.

Van strafbaarheid is alleen sprake als het opnemen van de communicatie wederrechtelijk is. Daardoor ontbreekt de strafbaarheid in bijvoorbeeld het geval van toestemming van de deelnemers aan de communicatie, maar ook in gevallen waarin het zonder toestemming/medeweten van een van de deelnemers opnemen van de communicatie civielrechtelijk niet onrechtmatig is, bijvoorbeeld in het uitzonderlijke geval dit noodzakelijk is om misstanden aan de kaak te stellen en dit belang zwaarder weegt dan de belangen die zijn gemoeid met de bescherming van de persoonlijke levenssfeer van de deelnemers aan de communicatie. Overigens is het openlijk opnemen van gesprekken in de openbare ruimte niet strafbaar. Dat verandert door dit wetsvoorstel – waarin de strafbaarheid wordt uitgebreid tot gesprekken waaraan de dader zelf deelneemt – niet.

5. Financiële paragraaf

PM

II. ARTIKELSGEWIJS

Artikel I, onderdeel A

Zoals in paragraaf 2 van het algemeen deel van de toelichting is opgemerkt, wordt de bevoegdheid van de officier van justitie om te vorderen dat gegevens ontoegankelijk worden gemaakt, als zelfstandige bevoegdheid opgenomen in het Wetboek van Strafvordering (zie nader artikel II, onderdeel B). De vervolgingsuitsluitingsgrond van artikel 54a Sr wordt – in het thans toegelichte onderdeel – gehandhaafd. Van de gelegenheid is gebruik gemaakt om deze vervolgingsuitsluitingsgrond op enkele punten te verhelderen en meer toe te snijden op de gedragscode "Notice and Take Down". Alvorens dit toe te lichten wordt aandacht geschonken aan de achtergrond van de vervolgingsuitsluitingsgrond.

Artikel 54a Sr vormde een onderdeel van de Aanpassingswet richtlijn inzake elektronische handel (Stb. 2004, 210). Met de inwerkingtreding van die wet is de Richtlijn inzake elektronische handel (2000/31/EG) geïmplementeerd. Die richtlijn beoogt binnen de Europese Unie een ruimte zonder binnengrenzen te scheppen voor diensten van de informatiemaatschappij. Onderdeel hiervan vormt de begrenzing van de aansprakelijkheid van dienstverleners van de informatiemaatschappij die als tussenpersoon optreden. De activiteiten van een intermediaire dienstverlener of tussenpersoon op het gebied van de opslag of doorgifte van gegevens kunnen namelijk worden gebruikt om onwettige informatie te ontsluiten. De uitwisseling van informatie kan strafbaar of onrechtmatig zijn op grond van de aard van de informatie, zoals bij uitings- en verspreidingsdelicten; de kwaliteit van de informatie, zoals in het geval van valsheid in geschrifte en oplichting; en de status van de informatie, zoals in het geval van auteursrechtschendingen en openbaarmaking van geheimen (Kamerstukken II 2001/02, 28 197, nr. 3, blz. 25). Afdeling 4 van de richtlijn behandelt de aansprakelijkheid van dienstverleners van de informatiemaatschappij die als tussenpersoon optreden. Het in de richtlijn opgenomen aansprakelijkheidssysteem heeft een horizontale strekking. Dat betekent dat de aansprakelijkheidsbepalingen van de richtlijn zowel op het strafrecht als het privaatrecht van toepassing zijn. De implementatie van de richtlijn heeft destijds daarom geleidt tot een aanpassing van zowel het Burgerlijk Wetboek als het Wetboek van Strafrecht. Kern van de aansprakelijkheidsregeling in de artikelen 12 tot en met 14 van de richtlijn is dat internetproviders niet aansprakelijk kunnen worden gehouden als zij geen actieve bemoeienis hebben met de gegevens die zij doorgeven, tijdelijk bewaren of opslaan of, zodra zij kennis krijgen van de onrechtmatigheid van de gegevens of activiteiten, prompt handelen om de gegevens of activiteiten ontoegankelijk te maken (Kamerstukken II 2001/02, 28 197, nr. 3, blz. 25). Daarbij maakt de richtlijn onderscheid tussen "mere conduit" (het doorgeven van gegevens of toegang verlenen tot een communicatienetwerk), "caching" (het tijdelijk opslaan van gegevens teneinde de doorgifte aan andere gebruikers van de dienst doeltreffender te maken), en "hosting"

(opslag van door een gebruiker van de dienst verstrekte gegevens). De vrijstelling van aansprakelijkheid heeft alleen betrekking op de doorgifte of opslag van informatie die voor het publiek toegankelijk is, bijvoorbeeld via websites of nieuwsgroepen.

Met de vervolgingsuitsluitingsgrond van artikel 54a Sr is – wat betreft het strafrecht – destijds gevolg gegeven aan de in de artikelen 12 tot en met 14 van de richtlijn neergelegde beperking van de aansprakelijkheid van de intermediaire dienstverlener van de informatiemaatschappij. Artikel 54a Sr voorziet erin dat vervolging is uitgesloten indien de tussenpersoon voldoet aan een bevel van de officier van justitie om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Zoals gezegd wordt de vervolgingsuitsluitingsgrond in dit onderdeel op een aantal punten verhelderd. Het geldende artikel 54a Sr kan de indruk wekken dat alleen het voldoen aan een vordering van de officier van justitie om de gegevens ontoegankelijk te maken vervolgingsuitsluitend werkt. Uit zowel de richtlijn als de memorie van toelichting bij het wetsvoorstel dat tot introductie van artikel 54a Sr heeft geleid, volgt echter dat de aanbieder die geen wetenschap heeft van het feit evenmin als zodanig kan worden vervolgd indien van een vordering van de officier van justitie geen sprake is. Daarom is bepaald dat de aanbieder die geen wetenschap heeft van het strafbaar feit als zodanig niet kan worden vervolgd.

Voorts is bepaald dat de aanbieder die weet heeft van het strafbaar feit en die onverwijld alle maatregelen neemt die redelijkerwijs van hem kunnen worden gevergd om de desbetreffende gegevens ontoegankelijk te maken, als zodanig niet kan worden vervolgd. Die wetenschap kan ontstaan doordat de aanbieder in het kader van de NTD-gedragscode is geattendeerd op de desbetreffende gegevens. Hierdoor kan het nieuwe artikel 54a Sr als een steun in de rug fungeren voor de NTD-gedragscode. Ook kan die wetenschap ontstaan door een vordering op grond van het voorgestelde artikel 125p Sv. Voor de duidelijkheid is, in lijn met het geldende artikel 54a Sr, expliciet bepaald dat voldoen aan een dergelijke vordering vervolging uitsluit. Dat door middel van zijn dienst een strafbaar feit wordt begaan moet voor de aanbieder buiten redelijke twijfel zijn. In geval slechts een kans bestaat dat zulks het geval is, is van “wetenschap” van een strafbaar feit geen sprake. De aanbieder die zich slechts bewust is van een kans dat een strafbaar feit wordt begaan, en die daarom de gegevens niet ontoegankelijk maakt, kan met andere woorden als zodanig niet worden vervolgd. Dit sluit aan bij de NTD-gedragscode waarin ontoegankelijkmaking van gegevens is voorzien indien “onmiskenbaar” sprake is van “strafbare inhoud”.

Opmerking verdient dat van een aanbieder van een communicatiedienst, die veelal grote hoeveelheden gegevens voor zijn afnemers verwerkt, niet kan worden verwacht dat

hij over diepgaande juridische expertise beschikt om te beoordelen of het om een strafbaar feit gaat. Ook uit de Richtlijn inzake elektronische handel, in het bijzonder de artikelen 14 en 15, blijkt dat de aanbieder geen algemene verplichting kan worden opgelegd om kennis te nemen van de gegevens die hij voor derden verwerkt of actief te zoeken naar strafbare feiten die met gebruikmaking van zijn dienst worden begaan. Een dergelijke algemene verplichting zou ook in strijd zijn met het verbod op preventieve censuur, dat voortvloeit uit artikel 10 EVRM en artikel 7 Grondwet. Dit betekent dat vervolging van de aanbieder alleen aan de orde kan zijn als hij nalaat gegevens ontoegankelijk te maken in gevallen waarin buiten redelijke twijfel is dat uitwisseling daarvan een strafbaar feit oplevert. Dit zal bijvoorbeeld het geval zijn bij afbeeldingen van kinderporno die op het internet zijn geplaatst, en waarbij over de leeftijd van het afgebeelde kind geen onduidelijkheid bestaat, of wanneer er een rechterlijke uitspraak is waarin de strafbaarheid van een identieke afbeelding is vastgesteld of waardoor het algemeen bekend is dat het een strafbare uiting betreft. Bij dit laatste kan bijvoorbeeld worden gedacht aan de publicatie van "Mein Kampf" van Adolf Hitler op het internet. Daarentegen zal bij uitingen waarbij de vrijheid van meningsuiting in het geding is, de strafbaarheid daarvan doorgaans niet door de aanbieder kunnen worden vastgesteld. In die gevallen waarbij twijfel kan bestaan over de strafbaarheid van een feit zal de officier van justitie eerst zelf een oordeel moeten vellen over de strafbaarheid. Als de officier van justitie ontoegankelijkmaking noodzakelijk acht, zal hij dit van de aanbieder kunnen vorderen op grond van het voorgestelde artikel 125p Sv. De aanbieder is gehouden aan de vordering te voldoen.

Het bestanddeel volgens hetwelk de aanbieder "als zodanig" moet hebben gehandeld, is gehandhaafd. Daaruit volgt dat de uitsluiting van vervolging niet absoluut is, maar alleen geldt in de hoedanigheid van een aanbieder van een communicatiedienst. De aanbieder die zelf een actieve bijdrage levert aan de strafbare feiten door middel van zijn dienst komt geen beroep op de vervolgingsuitsluitingsgrond toe (Hof Leeuwarden 20 april 2009, LJN BI1645).

Ook het bestanddeel "ontoegankelijk maken" is gehandhaafd. Zoals uit de memorie van toelichting bij het wetsvoorstel dat tot het geldende artikel 54a Sr heeft geleid is aangegeven, omvat het ontoegankelijk maken ook het verwijderen van gegevens, zij het met behoud van een kopie ten behoeve van de strafvordering (Kamerstukken II 2001/02, 28 197, nr. 3, blz. 65). Daarnaast kan het ontoegankelijk maken ook bestaan uit het filtreren of blokkeren van gegevens door de aanbieder.

Ten slotte wordt voorgesteld het bestanddeel "een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn" te vervangen door de term "aanbieder van een communicatiedienst". De laatstgenoemde term sluit aan bij de in het Wetboek van Strafrecht (zie artikel I, onderdeel B) en het Wetboek van Strafvordering (artikel 126la Sv)

gebruikelijke terminologie. Onder deze definitie vallen de dienstverleners en de door hen aangeboden diensten waar afdeling 4 van de Richtlijn inzake elektronische handel op ziet.

Artikel I, onderdeel B

Dit onderdeel betreft een omschrijving van het begrip "aanbieder van een communicatiedienst". Hiervoor is aangesloten bij de begripsomschrijving van artikel 126la Sv, dat een uitvloeisel vormt van de ratificatie van het Cybercrimeverdrag. In dat artikel is een aanbieder van een communicatiedienst gedefinieerd als: de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst. Deze begripsomschrijving omvat zowel de aanbieders van openbare telecommunicatiediensten als de aanbieders van besloten diensten of netwerken. Tevens vallen degenen hieronder die gegevens verwerken of opslaan ten behoeve van een communicatiedienst of diens gebruikers.

Artikel I, onderdelen C en D

Deze onderdelen zijn toegelicht in paragraaf 4 van het algemeen deel van de toelichting. Een bestanddeel van de in de geldende artikelen 139a, eerste lid, en 139b, eerste lid, Sr opgenomen delictsomschrijvingen is dat het afluisteren of opnemen anders dan in opdracht van een gespreksdeelnemer plaatsvindt. De bedoeling daarvan is dat het afluisteren of opnemen van een gesprek in opdracht van een van de gespreksdeelnemers niet strafbaar is. Een ander bestanddeel van beide delictsomschrijvingen is dat degene die het gesprek opneemt geen gespreksdeelnemer is. En het "afluisteren" van gesprekken, als verwoord in de beide delictsomschrijvingen, impliceert reeds dat degene die dat doet geen gespreksdeelnemer is. Gespreksdeelnemers zijn daardoor niet strafbaar. Om redenen die in paragraaf 4 zijn toegelicht wordt voorgesteld om de voorwaarde dat de dader geen gespreksdeelnemer is uit beide delictsomschrijvingen te schrappen.

In deze onderdelen wordt voorgesteld in de delictsomschrijvingen van de artikelen 139a, eerste lid, en 139b, eerste lid, Sr het bestanddeel "wederrechtelijk" op te nemen. In paragraaf 4 van het algemeen deel van de toelichting is een aantal voorbeelden gegeven van gevallen waarin het afluisteren of opnemen van een gesprek niet wederrechtelijk is. In aanvulling daarop moet worden opgemerkt dat het afluisteren of opnemen van een gesprek evenmin wederrechtelijk is als dit gebeurt door de rechtmatige toepassing van wettelijke bevoegdheden, zoals de bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering of bevoegdheden uit de Wet op de inlichtingen- en veiligheidsdiensten 2002.

In verband met de opneming van het bestanddeel wederrechtelijk in het eerste lid van de artikelen 139a en 139b Sr is handhaving van artikel 139a, tweede lid, onderdeel 3, Sr en de verwijzing in artikel 139b, tweede lid, Sr naar artikel 139a, tweede lid, onderdeel 3, Sr overbodig geworden. Artikel 139a, tweede lid, onderdeel 3, Sr noemt thans bovendien alleen de uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002 en kan daardoor – ten onrechte – de indruk wekken dat als gesprekken worden afgeluisterd of opgenomen door de rechtmatige toepassing van bevoegdheden uit het Wetboek van Strafvordering dit strafbaar zou zijn.

Ten overvloede kan er nog op worden gewezen dat als zonder toestemming van de gespreksdeelnemers in een woning gesprekken zijn opgenomen, de strafbaarheid nog kan ontbreken als het technische hulpmiddel op gezag van de gebruiker van de woning niet heimelijk aanwezig is, onder de voorwaarde dat geen sprake is van kennelijk misbruik (zie artikel 139a, tweede lid, onderdeel 2, Sr). En zoals in paragraaf 4 van het algemeen deel van de toelichting al werd aangestipt, is het afluisteren of opnemen van gesprekken die elders dan in een woning, besloten lokaal of erf worden gevoerd alleen strafbaar indien dit heimelijk geschiedt. Niet heimelijk opnemen of afluisteren is daardoor toegestaan; toestemming van de gespreksdeelnemers is in dat geval niet vereist.

Ten slotte wordt opgemerkt dat in de delictsomschrijvingen die in de beide onderdelen (C en D) worden voorgesteld, wordt gesproken over het "opzettelijk en wederrechtelijk" opnemen of afluisteren van gesprekken. Dit is de in het Wetboek van Strafrecht gebruikelijke formulering om uit te drukken dat het opzet van de dader niet ook is gericht op de omstandigheid dat het opnemen of afluisteren wederrechtelijk is.

Artikel I, onderdeel E

In dit onderdeel wordt artikel 139c, eerste lid, Sr gewijzigd. Voorgesteld wordt dit artikellid op te splitsen in een tweetal onderdelen (a en b). Onderdeel a is toegelicht in paragraaf 4 van het algemeen deel van de toelichting. Onderdeel b is toegelicht in paragraaf 3. Hieronder wordt in aanvulling daarop nader ingegaan op de voorgestelde wijzigingen, en wel per onderdeel.

Artikel 139c, eerste lid, aanhef en onder a, Sr

In het geldende artikel 139c, eerste lid, Sr wordt het wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van gegevens die door middel van telecommunicatie of een geautomatiseerd werk worden verwerkt of overgedragen, strafbaar gesteld. Bestanddeel van de delictsomschrijving is dat de gegevens niet bestemd zijn voor degene die deze aftapt of opneemt. Bij de toelichting op artikel I, onderdelen C en D, is – met

betrekking tot de daarin voorgestelde wijzigingen in de artikelen 139a en 139b Sr – aangegeven dat de desbetreffende delictsomschrijvingen worden verruimd, zodat ook het wederrechtelijk afluisteren of opnemen van een gesprek door een gespreksdeelnemer strafbaar is. Ditzelfde dient te gelden voor het opnemen of aftappen van een telefoongesprek of van andere gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of een geautomatiseerd werk, zoals een emailbericht. Ook in geval deze gegevens (mede) zijn bestemd voor degene die ze wederrechtelijk aftapt of opneemt, dient van strafbaarheid sprake te zijn. Ook voor dergelijke gegevens geldt dat de persoonlijke levenssfeer van de betrokkene in ernstige mate kan worden aangetast doordat de gegevens zonder zijn instemming worden afgetapt of opgenomen, al dan niet met het oog op de bekendmaking daarvan. In lijn met artikel 3 van het Cybercrimeverdrag is in de voorgestelde delictsomschrijving benadrukt dat het moet gaan om niet openbare gegevensoverdracht.

Het voorgaande heeft consequenties voor de inhoud van het bestanddeel "wederrechtelijk". Bij de wijziging van artikel 139c Sr door de Wet computercriminaliteit II is destijds aangegeven dat de uitsluiting van strafbaarheid van degene die in opdracht werkt van degene voor wie de gegevens (mede) bestemd zijn, geregeld wordt door de invoeging van het bestanddeel wederrechtelijk (Kamerstukken II 2004/05, 26 671, nr. 7, blz. 35). Met het schrappen van de woorden "die niet voor hem bestemd zijn" wordt hierin verandering gebracht. Ook degene die in opdracht handelt van degene voor wie de gegevens (mede) bestemd zijn, is voortaan strafbaar. Dit kan anders zijn als de deelnemers aan de communicatie toestemming hebben gegeven voor het opnemen of aftappen daarvan. Voorts is de gelegenheid te baat genomen om, in lijn met de hierboven bij artikel I, onderdelen C en D, toegelichte wijzigingen in de artikelen 139a en 139b Sr, ook de in artikel 139c Sr opgenomen expliciete uitzondering die inhoudt dat de strafbepaling niet van toepassing is als wordt afgetapt of opgenomen ten behoeve van de strafvordering of ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002, te schrappen. In geval wordt afgetapt of opgenomen door de rechtmatige toepassing van wettelijke bevoegdheden zijn deze handelingen niet wederrechtelijk en vallen om die reden buiten de reikwijdte van de delictsomschrijving. In paragraaf 4 van het algemeen deel van de toelichting zijn overigens enkele andere voorbeelden gegeven van gevallen waarin het wederrechtelijke karakter aan het opnemen of aftappen van die communicatie kan komen te ontvallen.

Artikel 139c, eerste lid, aanhef en onder b, Sr

In het voorgestelde artikel 139c, eerste lid, onderdeel b, Sr wordt voorzien in een zelfstandige strafbaarstelling van het wederrechtelijk overnemen van gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, zonder dat er – zoals bij

computervredebreuk – sprake behoeft te zijn van het binnendringen van het desbetreffende geautomatiseerde werk door degene die de gegevens (vervolgens) wederrechtelijk overneemt. Dit kan het geval zijn als de dader rechtmatige toegang heeft tot de gegevens van een computer, en daarvan misbruik maakt door de gegevens te kopiëren bijvoorbeeld met de bedoeling die gegevens aan derden te verkopen. Er is dus een actief handelen van de dader vereist. Uit het gebruik van het bestanddeel overnemen volgt dat niet vereist is dat de beschikkingsmacht van de rechthebbende wordt beperkt. Kenmerkend voor gegevens is dat zij kunnen worden gekopieerd zonder dat de rechthebbende de beschikkingsmacht over die gegevens verliest. Op dit punt is in paragraaf 3 van het algemeen deel van de toelichting al ingegaan. Het overnemen van de gegevens dient voorts opzettelijk te geschieden. De dader moet de niet voor hem bestemde gegevens dus willens en wetens overnemen.

Het overnemen van de gegevens dient daarnaast wederrechtelijk te zijn. Door het bestanddeel wederrechtelijk is verzekerd dat het overnemen van gegevens met toestemming van de rechthebbende niet strafbaar is. Evenmin is strafbaar de ambtenaar die door het overnemen van de gegevens op rechtmatige wijze uitvoering geeft aan wettelijke bevoegdheden, zoals bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering of bevoegdheden uit de Wet op de inlichtingen– en veiligheidsdiensten 2002.

Het moet gaan om gegevens die niet openbaar zijn. Voorkomen moet worden dat het van het internet downloaden van de hier aan de orde zijnde gegevens in het algemeen strafbaar wordt gesteld. Van strafbaarheid van downloaden is alleen sprake als bijzonder bepalingen daarin voorzien. Zo is het downloaden van afbeeldingen van kinderporno strafbaar op grond van artikel 240b Sr. En het downloaden van auteursrechtelijk beschermde gegevens is, voor zover dit niet onder het “thuiskopiestelsel” in artikel 16c e.v. van de Auteurswet valt, strafbaar op grond van de Auteurswet. De vraag of en zo ja onder welke voorwaarden het aangewezen is om in de toekomst het downloaden van auteursrechtelijk beschermd materiaal als onrechtmatig aan te merken of strafbaar te stellen – welke vraag aan de orde komt in kabinetsreactie op het rapport parlementaire werkgroep auteursrecht (Kamerstukken II 2009/10, 29 838, nr. 22, paragraaf 5) – is een kwestie die door het auteursrecht wordt beheerst en in dat kader moet worden bezien.

Artikel I, onderdeel F

In het geldende artikel 139e Sr worden drie verschillende gedragingen strafbaar gesteld, te weten: het beschikken over een voorwerp waarop gegevens zijn vastgelegd die door middel van het afluisteren, aftappen of opnemen van een gesprek, van telecommunicatie of van andere gegevensoverdracht of –verwerking zijn verkregen (onderdeel 1), het ter beschikking stellen van een dergelijk voorwerp aan anderen (onderdeel 3) en het bekend

maken van gegevens die zijn verkregen door middel van het afluisteren, aftappen of opnemen van een gesprek, van telecommunicatie of van andere gegevensoverdracht of –verwerking (onderdeel 2). In paragraaf 3 van het algemeen deel van de toelichting is reeds stilgestaan bij de noodzaak om de strafrechtelijke bescherming van computergegevens te verbeteren. Daartoe wordt in artikel I, onderdeel E, voorgesteld artikel 139c Sr aan te vullen zodat ook het overnemen van gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, zonder dat er sprake is van het binnendringen van dat werk door degene die de gegevens wederrechtelijk overneemt, strafbaar is. In het verlengde hiervan wordt in dit onderdeel voorgesteld om ook artikel 139e Sr aan te vullen zodat degene die over wederrechtelijk overgenomen gegevens beschikt en weet of redelijkerwijs moet vermoeden dat het om zulke gegevens gaat, eveneens strafbaar is. Vereist is dat de dader weet of redelijkerwijs moet vermoeden dat de gegevens door wederrechtelijk overnemen zijn verkregen. Als de gegevens aan een derde ter hand worden gesteld, dan is deze op zijn beurt strafbaar voor het beschikken over deze gegevens indien hij weet of redelijkerwijs moet vermoeden dat het om zulke gegevens gaat.

In het voorgestelde artikel 139e Sr is opgenomen dat het moet gaan om niet openbare gegevens. Zonder deze beperking zou het van het internet downloaden van gegevens die eerder wederrechtelijk zijn overgenomen in het algemeen strafbaar worden. Voor bepaalde gegevens, zoals afbeeldingen van kinderporno en auteursrechtelijk beschermd materiaal dat niet onder het thuiskopiestelsel valt, is downloaden overigens uit anderen hoofde strafbaar.

In dit onderdeel wordt voorts het bestanddeel “voorwerp” uit artikel 139e Sr geschrapt. Door niet te verwijzen naar de gegevensdrager waarop de gegevens zijn vastgelegd, wordt zekergesteld dat niet alleen het beschikken over gegevens die op een usb-stick of een portable harde schijf staan strafbaar is, maar ook het beschikken over gegevens die op een emailaccount staan.

Voorts wordt in dit onderdeel de maximale gevangenisstraf verhoogd van zes maanden naar een jaar. Deze wijziging is toegelicht in paragraaf 3 van het algemeen deel.

Ten slotte is van de gelegenheid gebruik gemaakt om enkele redactionele vereenvoudigingen in artikel 139e Sr door te voeren. Het aan een ander ter beschikking stellen en bekend maken zijn samengevoegd in onderdeel b van het voorgestelde artikel 139e Sr. Ongewijzigd blijft dat het bekend maken aan een ander strafbaar is zowel in geval de dader de gegevens zelf eerder wederrechtelijk heeft afgeluisterd, afgetapt of opgenomen (of overgenomen) als in geval een ander dat heeft gedaan.

Artikel II, onderdeel A

Uit een oogpunt van wetssystematiek ligt het voor de hand om de bevoegdheid van de officier van justitie te vorderen dat gegevens ontoegankelijk worden gemaakt te plaatsen in het Eerste Boek, Titel IV, van het Wetboek van Strafvordering, waarin de dwangmiddelen zijn opgenomen. Voorgesteld wordt de bevoegdheden betreffende het ontoegankelijk maken van gegevens in een afzonderlijke afdeling op te nemen. Het betreft de bestaande bevoegdheid om bij gelegenheid van een doorzoeking aangetroffen gegevens ontoegankelijk te maken (artikel 125o Sv) alsmede de in dit wetsvoorstel voorgestelde bevoegdheden betreffende het vorderen dat gegevens ontoegankelijk worden gemaakt (de voorgestelde artikelen 125p en 125q Sv).

Artikel II, onderdeel B

In dit onderdeel wordt voorgesteld twee artikelen – 125p en 125q – aan het Wetboek van Strafvordering toe te voegen. Deze artikelen worden – in aanvulling op paragraaf 2 van het algemeen deel van de toelichting – hieronder nader toegelicht.

Artikel 125p Sv

Eerste lid

Het eerste lid bepaalt dat de officier van justitie van de aanbieder van een communicatiedienst of van degene die de beschikkingsmacht heeft over het geautomatiseerde werk kan vorderen om onverwijld alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven ontoegankelijk te maken, teneinde een strafbaar feit te beëindigen of nieuwe strafbare feiten te voorkomen. De vordering is een dwangmiddel dat is bedoeld om strafbare feiten die met behulp van een geautomatiseerd werk worden begaan te beëindigen of te voorkomen. Doorgaans kan de politie door middel van feitelijk optreden strafbare feiten beëindigen of nieuwe strafbare feiten voorkomen, door bijvoorbeeld voorwerpen in beslag te nemen of personen aan te houden en in verzekering te stellen. Bij de beëindiging van strafbare feiten met behulp van een geautomatiseerd werk is echter in veel gevallen de medewerking van een derde vereist die de beschikkingsmacht heeft over de gegevens die op het internet zijn geplaatst of in een computer zijn opgeslagen. Het bevel kan daarom, behalve aan de aanbieder van een communicatiedienst, ook worden gericht tot degene die de beschikking heeft over het geautomatiseerde werk met gebruikmaking waarvan het strafbare feit wordt begaan. Dat is degene die een website op het internet geplaatst heeft en die in staat moet worden geacht die website aan te passen of de inhoud daarvan van het internet te verwijderen.

De bevoegdheid tot het doen van de vordering is – ook thans – belegd bij de officier van justitie. Gelet op de aard van de vordering en de rol van de officier van justitie bij de beoordeling van strafbare feiten, is hij de meest aangewezen functionaris om deze bevoegdheid toe te passen. Hoewel de politie eveneens tot taak heeft strafbare feiten te beëindigen en te voorkomen, is de bevoegdheid te vorderen dat gegevens ontoegankelijk worden gemaakt voorbehouden aan de officier van justitie. Aangezien bij het ontoegankelijk maken van gegevens op het internet terughoudendheid moet worden betracht teneinde onrechtmatige inperkingen van de vrijheid van meningsuiting en het vrije verkeer van gegevens te voorkomen, is niet wenselijk dat deze bevoegdheid ook aan opsporingsambtenaren wordt toebedeeld. In het bijzonder bij uitingsdelicten is diepgaande juridische expertise vereist om snel tot een afgewogen oordeel ten aanzien van de strafbaarheid van de gedraging te komen, zodat opgetreden kan worden om de gegevens ontoegankelijk te maken. Het is van belang dat binnen het Openbaar Ministerie gespecialiseerde officieren van justitie zijn aangewezen die zijn belast met de beoordeling van de strafbaarheid van de gedragingen op het internet en de wenselijkheid van een vordering op grond van dit artikel te doen. Dit dient op landelijk niveau te zijn georganiseerd zodat de nodige expertise kan worden opgebouwd, een eenduidig beleid kan worden ontwikkeld, ook in de richting van de aanbieders van internetdiensten, en vierentwintiguurs beschikbaarheid kan worden verzekerd.

Zoals in paragraaf 2 van het algemeen deel van de toelichting uiteen is gezet, bestaat er geen noodzaak om het (in het geldende artikel 54a Sr opgenomen) vereiste van de voorafgaande machtiging van de rechter-commissaris te handhaven. De vordering tot het ontoegankelijk maken van gegevens is een maatregel van tijdelijke aard. Over de vordering kan bovendien beklag worden gedaan bij de raadkamer van de rechtbank. Het is aan de rechter om te beslissen of de gegevens waarop de vordering betrekking heeft, al dan niet moeten worden vernietigd. In het geval niet aan de vordering wordt voldaan en daarvoor op grond van artikel 184 Sr strafvervolging wordt ingesteld, zal de rechter beoordelen of de vordering rechtmatig is gedaan. In dit licht is toetsing door de rechter voldoende gewaarborgd. Handhaving van voorafgaande machtiging door de rechter-commissaris is daarom niet noodzakelijk.

Overigens kent het civiele recht al bijzondere procedures om onrechtmatige activiteiten snel te kunnen beëindigen. Zo biedt het Wetboek van Burgerlijke Rechtsvordering een regeling om inbreuken op intellectueel eigendom snel en effectief aan te pakken (artikel 1019 e.v. Rv). Deze regeling maakt het mogelijk dat de rechtbank, in sommige gevallen zelfs binnen een uur nadat een verzoek daartoe is binnengekomen, de gedaagde partij beveelt om de onrechtmatige activiteiten te beëindigen. Teneinde de snelheid van deze procedure te waarborgen, zijn deze zaken geconcentreerd bij de Rechtbank Den Haag. Tevens kan worden gewezen op de speciale procedures in de

Auteurswet (artikel 26d) en de Wet op de naburige rechten (artikel 15e), waarbij de rechter kan worden verzocht om een internetprovider te bevelen om de inbreukmakende activiteiten van derden te staken. Dit wetsvoorstel sluit daarbij aan door de bestaande strafrechtelijke bevoegdheid van de officier van justitie om te bevelen gegevens ontoegankelijk te maken, te versterken.

Een kenmerk van het internet is dat informatie razendsnel kan worden verspreid en met een groot publiek gedeeld kan worden. Indien gegevens eenmaal op het internet zijn geplaatst is het buitengewoon moeilijk deze gegevens als zij door middel het internet zijn verspreid, daarvan geheel te verwijderen. Daarom is het van belang dat, in de gevallen waarin daartoe aanleiding bestaat, snel kan worden ingegrepen om de schadelijke effecten zoveel mogelijk te beperken. Dit komt ook tot uitdrukking in de Richtlijn inzake elektronische handel die ervan uitgaat dat de aanbieder van een hosting-dienst alleen dan niet aansprakelijk is indien hij, zodra hij daadwerkelijk kennis heeft of krijgt, "prompt" handelt om de informatie te verwijderen of de gegevens ontoegankelijk te maken. In lijn daarmee wordt in het eerste lid bepaald dat de aanbieder gehouden is "onverwijld" alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens ontoegankelijk te maken. Met het gebruik van de term "onverwijld" wordt tot uitdrukking gebracht dat van de aanbieder van een communicatiedienst of degene die de beschikkingsmacht heeft over een geautomatiseerd werk wordt verwacht dat deze zo snel mogelijk alle maatregelen neemt die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken, ter beëindiging van een strafbaar feit of ter voorkoming van strafbare feiten.

Op grond van het derde lid wordt onder het "ontoegankelijk maken" van gegevens hetzelfde verstaan als in het geldende artikel 125o Sv, te weten: het treffen van maatregelen (zoals filteren of blokkeren) ter voorkoming dat de beheerder van een geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Dit betekent dat ook het verwijderen van de gegevens met behoud van een kopie ten behoeve van de strafvordering, besloten ligt in het begrip "ontoegankelijk maken". Aangezien het in bepaalde gevallen technisch niet goed mogelijk kan zijn om de gegevens effectief ontoegankelijk te maken, is de verplichting tot het ontoegankelijk maken, evenals in het geldende artikel 54a Sr het geval is, in het eerste lid geclausuleerd. Van de aanbieder of degene die de beschikkingsmacht heeft over het geautomatiseerd werk, wordt verlangd dat hij alle maatregelen neemt "die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken". De officier van justitie kan indien de gegevens niet ontoegankelijk worden gemaakt en hij gegronde redenen heeft om aan te nemen dat degene tot wie de vordering is gericht, zich onvoldoende heeft ingespannen om de

gegevens ontoegankelijk te maken, hem zo nodig vervolgen voor het niet voldoen aan een ambtelijk bevel (artikel 184 Sr) dan wel voor het begaan van het strafbaar feit waarop de gegevens, waarvan de ontoegankelijkmaking is gevorderd, betrekking hebben.

Het eerste lid laat overigens de mogelijkheid onverlet dat de officier van justitie besluit de strafbare feiten te beëindigen door middel van een doorzoeking ter vastlegging van gegevens. Op grond van artikel 125i, eerste lid, Sv kan, onder de in dat artikellid bedoelde voorwaarden, een plaats worden doorzocht ter vastlegging van gegevens die op die plaats op een gegevensdrager zijn vastgelegd of opgeslagen. Indien bij de doorzoeking gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is begaan, kan de officier van justitie op grond van artikel 125o, eerste lid, Sv bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming daarvan.

Tweede lid

De vordering dient op schrift te worden gesteld en moet voldoen aan een aantal eisen die in het tweede lid worden opgesomd. Allereerst zal de vordering duidelijk moeten maken welk strafbaar feit het betreft en zo mogelijk de naam van de verdachte. Gelet op de mogelijkheden die het internet biedt om de werkelijke identiteit te verhullen, zal het niet altijd mogelijk zijn om de (identiteit van de) verdachte te achterhalen. In dat geval kan worden volstaan met een zo nauwkeurige mogelijke aanduiding (onderdeel a).

De vordering zal ook duidelijkheid moeten verschaffen over de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens nodig is om een strafbaar feit te beëindigen of strafbare feiten te voorkomen (onderdeel b). Om te voorkomen dat de vrijheid van meningsuiting verder dan noodzakelijk wordt ingeperkt, zal de officier van justitie nauwkeurig moeten bepalen welke gegevens een strafbaar feit behelzen en – dus – ontoegankelijk moeten worden gemaakt door degene tot wie de vordering is gericht (onderdeel c). Dit kan geschieden aan de hand van IP-adressen. De officier van justitie zal hierbij rekening moeten houden met de technische mogelijkheden om onderdelen van pagina’s of websites te kunnen verwijderen. Voorkomen moet worden dat tot de aanbieder een vordering wordt gericht die technisch niet kan worden uitgevoerd.

Als de officier van justitie een dwangsom wil opleggen voor het niet of niet tijdig voldoen aan de vordering, zal dit ook in het bevel tot uitdrukking moeten komen (onderdeel d). Zie hierover de toelichting op het voorgestelde artikel 125q Sv.

Derde lid

In het derde lid wordt artikel 125o, tweede en derde lid, Sv van overeenkomstige toepassing verklaard. Artikel 125o, tweede lid, Sv bevat een omschrijving van het begrip ontoegankelijk maken van gegevens. Op dit begrip is hierboven, bij de toelichting op het eerste lid, reeds ingegaan. De bevoegdheid tot het doen van een vordering op grond van het eerste lid komt aan de officier van justitie toe zodra hij tot het oordeel komt dat er sprake is van een strafbaar feit door middel van een geautomatiseerd werk. Doordat artikel 125o, derde lid, Sv van overeenkomstige toepassing is verklaard, is erin voorzien dat, zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregel van de ontoegankelijkmaking, de officier van justitie bepaalt dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerde werk worden gesteld.

Artikel 125q Sv

Naar analogie van de regeling voor het ontoegankelijk maken van activiteiten of gegevens waarmee een inbreuk wordt gemaakt op het intellectueel eigendomsrecht (artikel 1019 e.v. Rv), biedt dit artikel de mogelijkheid dat in de vordering tot het ontoegankelijk maken van gegevens een dwangsom kan worden opgelegd voor het niet of niet tijdig voldoen aan de vordering. Met de bevoegdheid voor de officier van justitie tot het opleggen van een dwangsom wordt aangesloten bij het bestuursrecht. De Algemene wet bestuursrecht (Awb) kent een bestuursorgaan dat bevoegd is een last onder bestuursdwang op te leggen de bevoegdheid toe om in plaats daarvan een last onder dwangsom op te leggen (artikel 5:32 Awb). Onder een last onder dwangsom wordt verstaan de herstelsanctie inhoudende een last tot geheel of gedeeltelijk herstel van de overtreding en de verplichting tot betaling van een geldsom indien de last niet of niet tijdig wordt uitgevoerd (artikel 5:31d Awb). De dwangsombevoegdheid houdt in dat een last wordt gegeven tot beëindiging en/of het niet voortzetten van of herhalen van een overtreding. Bij het niet of niet geheel uitvoeren van de last worden een of meer geldsommen verbeurd. De bedoeling van een last onder dwangsom is dat de verschuldigdheid van de dwangsom wordt voorkomen doordat de dreiging daarvan bewerkstelligt dat de overtreder de overtreding beëindigt.

In het strafrecht is tot dusver niet voorzien in de mogelijkheid van een dwangsom voor het niet of niet tijdig opvolgen van een strafvorderlijk bevel. In het WODC-rapport "De WED op de helling" (Den Haag, 2005, blz. 150 e.v.) wordt geconstateerd dat het sanctiepakket van de Wet op de economische delicten herijking behoeft. De onderzoekers wijzen erop dat een last onder dwangsom, wat betreft effectiviteit en doelmatigheid de voorkeur geniet bij spoedeisende maatregelen boven een vervolging voor het niet opvolgen van een bevel. In de beleidsreactie op dit rapport is de aanbeveling overgenomen om een last onder dwangsom mogelijk te maken voor de handhaving van de economische wetgeving. Daarbij is aangegeven dat oplegging van de last onder dwangsom niet alleen

aan de strafrechter, maar ook – in het kader van de strafbeschikking – aan het Openbaar Ministerie zou kunnen worden toegestaan (Kamerstukken II 2006/07, 30 800 VI, nr. 90, blz. 8). Aan deze aanbeveling is nog niet in algemene zin uitvoering gegeven.

Er bestaat aanleiding om aan de officier van justitie een dwangsombevoegdheid toe te kennen voor het geval een aanbieder niet voldoet aan een vordering van de officier van justitie tot het ontoegankelijk maken van gegevens. In een dergelijk geval kan de officier van justitie weliswaar overgaan tot vervolging wegens het niet nakomen van een bevoegd gegeven ambtelijk bevel (artikel 184 Sr), maar een last onder dwangsom kan – gelet op de tijd die pleegt te verstrijken met een afgeronde strafvervolging en gelet op het betrekkelijk lage geldboetemaximum dat bij artikel 184 Sr is voorzien (te weten: die van de tweede categorie) – doelmatiger zijn. Daarbij kan worden gedacht aan gevallen van bedreiging via een communicatiedienst van personen of het op het internet tonen van afbeeldingen die de rechtsorde schokken, maar ook aan gevallen waarin de maximale geldboete wegens het niet voldoen aan de vordering niet in verhouding zou staan tot de mogelijke gevolgen van de strafbare feiten die door middel van de communicatiedienst worden begaan.

Het is om deze redenen dan ook gewenst de officier van justitie de bevoegdheid toe te kennen om ontoegankelijkmaking af te dwingen door het opleggen van een dwangsom. In de vordering kan de officier van justitie bepalen dat per tijdseenheid waarin niet aan de vordering is voldaan, een oplopende dwangsom wordt verbeurd. Deze aanpak sluit aan bij de mogelijkheden die het privaatrecht kent, zoals deze in de artikelsgewijze toelichting op het voorgestelde artikel 125p Sv al aan de orde kwamen. Oplegging van een dwangsom is alleen aan de orde in gevallen die daartoe aanleiding geven. Gelet op de medewerking van de internetproviders aan de NTD-gedragscode en aan de bereidwilligheid van internetproviders om mee te werken aan strafvorderlijke bevelen, zal er in de praktijk niet snel reden zijn om aan aanbieders van een communicatiedienst een dwangsom op te leggen. Zoals hierboven echter reeds is uiteen gezet, kunnen er situaties zijn waarin daaraan wel behoefte bestaat.

Nu de Algemene wet bestuursrecht een uitgebreide regeling kent voor het opleggen van een last onder dwangsom, is ervoor gekozen om deze regeling van overeenkomstige toepassing te verklaren op de door de officier van justitie opgelegde dwangsom wegens het niet voldoen aan de vordering tot het ontoegankelijk maken van gegevens. Dit met uitzondering van het tegen de oplegging van een dwangsom in te stellen rechtsmiddel. Op grond van artikel 552a Sv kan een belanghebbende zich beklagen over de inbeslagneming van voorwerpen. Deze procedure is, naar wordt voorgesteld en hierboven is toegelicht, eveneens van toepassing indien de betrokkene beklag wil doen over de vordering tot het ontoegankelijk maken van gegevens op grond van artikel 125p Sv. Het ligt in de rede om voor de rechtsbescherming tegen een beslissing tot oplegging van een dwangsom bij deze procedure aan te sluiten. Voorgesteld wordt artikel 552a Sv aan te passen zodat ook tegen

een besluit tot oplegging van een dwangsom beklag kan worden gedaan bij de (straf)rechter.

Eerste en tweede lid

De procedure van oplegging van een dwangsom is als volgt. De officier van justitie kan op grond van het eerste lid in de vordering tot het ontoegankelijk maken van gegevens een dwangsom opnemen. Voor de omschrijving van het begrip dwangsom in het tweede lid is aangesloten bij de begripsomschrijving van artikel 5:31d Awb. Het gaat om een verplichting tot betaling van een geldsom indien niet aan de vordering om gegevens ontoegankelijk te maken wordt voldaan. Voordat de officier van justitie de vordering doet en de dwangsom oplegt dient hij de in het geding zijnde belangen af te wegen. Het betreft de belangen die zijn gediend bij strafrechtelijke rechtshandhaving en de belangen van degene die de gegevens op het internet wil publiceren. Omdat de officier van justitie alleen overgaat tot het doen van een vordering in gevallen waarin een spoedeisend belang aanwezig is bij het beëindigen van het strafbare feit is niet voorgeschreven dat, voordat de beschikking wordt gegeven, de belanghebbende dient te worden gehoord (vgl. artikel 4:8 Awb), mede omdat veelal sprake is van situaties die vallen binnen het kader van de NTD-gedragscode, en het nodige overleg met de aanbieder dan reeds is gevoerd.

Derde en vierde lid

De dwangsom wordt op grond van het vierde lid vastgesteld op een bedrag ineens of een bedrag per tijdseenheid waarin niet aan de vordering is voldaan. Ook moet in de vordering de maximaal te verbeuren dwangsom worden opgenomen. Het vastgestelde bedrag dient in een redelijke verhouding te staan tot de zwaarte van het geschonden belang en de beoogde werking van de dwangsomoplegging. In de beschikking dient een termijn te worden geboden waarbinnen degene tot wie de vordering is gericht daaraan kan voldoen en daarmee kan voorkomen dat de dwangsom daadwerkelijk verbeurd wordt. Dit wordt in het bestuursrecht wel de begunstigingstermijn genoemd. De gestelde termijn moet in de omstandigheden van het geval redelijk zijn en moet in ieder geval voldoende lang zijn om degene tot wie de vordering is gericht daadwerkelijk in staat te stellen daaraan te voldoen. De te beschermen belangen kunnen vereisen dat de termijn tot enkele dagen of zelfs uren wordt beperkt. Dit zal mede afhangen van de ernst van het strafbare feit en de duur en intensiteit van het met de aanbieder gevoerde overleg. Hierbij kan nog worden opgemerkt dat de termijn gedurende welke aan de vordering kan worden voldaan zonder dat een dwangsom wordt verbeurd, door de officier van justitie zo kort mogelijk moet worden gehouden.

Vijfde lid

In het vijfde lid worden enkele bepalingen betreffende de last onder dwangsom uit de Algemene wet bestuursrecht van overeenkomstige toepassing verklaard. Als bij de afloop van de termijn niet aan de vordering is voldaan, wordt de opgelegde dwangsom van rechtswege verbeurd. Alsdan ontstaat de verplichting tot betaling binnen zes weken na de verbeurte (artikel 5:33 Awb). De mogelijkheid bestaat om de vordering op verzoek van degene tot wie zij is gericht op te heffen of aan te passen, bijvoorbeeld in geval een aanbieder wegens overmacht niet aan de vordering kan voldoen (artikel 5:34, eerste lid, Awb). De invordering bij dwangbevel is geregeld in de Algemene wet bestuursrecht. De bevoegdheid tot uitvaardiging van een dwangbevel bestaat slechts indien zij bij de wet is toegekend (artikel 4:115 Awb). Deze bevoegdheid wordt in het vijfde lid aan de officier van justitie toebedeeld. Als de opgelegde dwangsom niet binnen twee weken wordt betaald dan zal de officier van justitie een dwangbevel uit kunnen doen gaan. Onder een dwangbevel wordt verstaan een schriftelijk bevel van een bestuursorgaan dat ertoe strekt de betaling van een geldsom af te dwingen (artikel 4:114 Awb). Eerst is een aanmaning vereist tot betaling binnen een korte termijn (artikel 4:112, eerste lid, Awb). De termijn waarbinnen de schuldenaar alsnog kan betalen is twee weken. Daarmee komt de totale termijn voor de betaling dus op acht weken, na het tijdstip van de verbeurte. Voorafgaand aan het doen uitgaan van de aanmaning behoeft de schuldenaar niet te worden gehoord (artikel 4:118 Awb). Indien de schuldenaar na het verstrijken van de termijn nog niet heeft betaald, is de officier van justitie bevoegd tot invordering over te gaan. Een dwangbevel wordt schriftelijk uitgevaardigd en levert een executoriale titel op in de zin van artikel 430 Rv die met toepassing van de voorschriften van het Wetboek van Burgerlijke Rechtsvordering ten uitvoer kan worden gelegd (artikel 4:116 Awb).

De regels over de invordering van de aanmaningsvergoeding, de wettelijke rente en de kosten van het dwangbevel zijn niet van toepassing (artikel 4:119, eerste lid, Awb). Dit betreft een regeling waarmee een officier van justitie minder vertrouwd is en die naar verwachting in de praktijk weinig zal worden toegepast. Wel van toepassing is de bepaling dat de kosten van de executie ten laste komen van de geëxecuteerde (artikel 4:120, eerste lid, Awb). De gerechtelijke kosten worden berekend met toepassing van de op grond van artikel 434a Rv vastgestelde tarieven (artikel 4:120, tweede lid, Awb). Dit is uitgewerkt in het Besluit tarieven ambtshandelingen gerechtsdeurwaarders. Over de buitengerechtelijke kosten is in het Besluit buitengerechtelijke kosten geregeld dat deze kosten in rekening kunnen worden gebracht voor zover zij redelijk zijn, met een maximum van vijftien procent van de te betalen geldsom (artikel 1 Besluit buitengerechtelijke kosten). De bekendmaking van het dwangbevel geschiedt door middel van de betekening van een exploot door een

deurwaarder (artikel 4:123, eerste lid, Awb). Met het dwangbevel wordt doorgaans tegelijkertijd een bevel tot betaling binnen twee dagen gedaan. Indien niet wordt betaald kan door de deurwaarder beslag worden gelegd op roerende of onroerende zaken of onder derden. Tegen het dwangbevel en de tenuitvoerlegging ervan kan worden opgekomen overeenkomstig de artikelen 438 en 438a Rv (artikel 4:123, eerste lid, Awb). De burgerlijke rechter is terzake bevoegd. Tegen een dwangbevel staan geen bezwaar en beroep open in de zin van de Algemene wet bestuursrecht (artikel 4:118 Awb).

Zesde lid

In het zesde lid wordt de mogelijkheid geboden om bij algemene maatregel van bestuur nadere regels te geven over de tenuitvoerlegging. Het ligt voor de hand om het Centraal Justitieel Incasso Bureau (CJIB) in schakelen voor de invordering van een opgelegde dwangsom. Het CJIB is reeds belast met inning van opgelegde sancties, ter ondersteuning van het Openbaar Ministerie. Dit betreft onder meer de inning van geldboetes en schadevergoedingsmaatregelen (artikel 572 Sv) en ontnemingsmaatregelen (artikel 577b Sv).

Het Wetboek van Strafvordering voorziet in een procedure voor het nemen van verhaal op voorwerpen door middel van een dwangbevel (artikel 575 Sv). Daarnaast kan verhaal zonder dwangbevel worden genomen op (met name) banktegoeden waarover de aanbieder beschikt (artikel 576 Sv). Overwogen kan worden om de procedure van artikel 576 Sv van overeenkomstige toepassing te verklaren op de invordering van een verbeurde dwangsom. Daarmee zou een eenduidige regeling worden verkregen voor het verhaal ten behoeve van de tenuitvoerlegging door het Openbaar Ministerie van een opgelegde sanctie.

Artikel II, onderdeel C

Dit onderdeel strekt ter reparatie van artikel 126bb Sv. Het betreft de mededelingsplicht van de officier van justitie met betrekking tot de toepassing van bijzondere opsporingsbevoegdheden. In het tweede lid, onderdeel b, van dit artikel wordt verwezen naar de artikelen 126m en 126t, derde lid, onderdeel c, Sv. Dit moet echter zijn de artikelen 126m en 126t, tweede lid, onderdeel c, Sv. In dit onderdeel wordt deze omissie hersteld.

Artikel II, onderdeel D

Dit onderdeel betreft de invoeging van twee artikelen in het Wetboek van Strafvordering, waarin begripsomschrijvingen zijn opgenomen.

In het voorgestelde artikel 138e Sv is een omschrijving opgenomen van het begrip "gegevens". Dit begrip wordt in veel bepalingen van het Wetboek van Strafvordering gebruikt, waaronder in het voorgestelde artikel 125p Sv. De omschrijving is gelijk aan die van artikel 80quinquies Sr.

In het voorgestelde artikel 138f Sv is een omschrijving opgenomen van het begrip "geautomatiseerd werk". Dit begrip wordt eveneens gebruikt in verschillende bepalingen van het Wetboek van Strafvordering, waaronder in het voorgestelde artikel 125p Sv. De omschrijving is gelijk aan die van artikel 80sexies Sr. Tijdens de mondelinge behandeling in de Eerste Kamer van het wetsvoorstel dat aan de Wet computercriminaliteit II ten grondslag ligt, is toegezegd bij een latere gelegenheid te zullen bezien in hoeverre er aanleiding is tot het opnemen van termen als "gegevens" en "geautomatiseerd werk" het Wetboek van Strafvordering (Handelingen I 2005/06, blz. 1351). Hiermee wordt uitvoering gegeven aan die toezegging.

Artikel II, onderdeel E

In artikel 354, eerste lid, Sv wordt geregeld dat in het geval dat de rechtbank een veroordeling, vrijspraak of ontslag van alle rechtsvervolging uitspreekt, tevens een beslissing wordt genomen over de met de toepassing van artikel 125o Sv ontoegankelijk gemaakte gegevens indien de desbetreffende maatregelen nog niet zijn opgeheven. 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 geautomatiseerde werk worden gesteld. Het ligt in de rede om deze procedure eveneens toe te passen in de gevallen waarin de officier van justitie op grond van het voorgestelde artikel 125p Sv een vordering tot ontoegankelijkmaking van de gegevens heeft gericht tot de aanbieder van een communicatiedienst of degene die de beschikkingsmacht heeft over het geautomatiseerde werk. Omdat deze procedure uitsluitend aan de orde zal kunnen zijn in die gevallen waarin de aanbieder zelf wordt vervolgd voor betrokkenheid bij een strafbaar feit ligt het in de lijn der verwachting dat deze procedure in de praktijk niet vaak toegepast zal worden. In de gevallen waarin de aanbieder niet vervolgd wordt maar de vernietiging van de ontoegankelijk gemaakte gegevens nodig is om nieuwe strafbare feiten te voorkomen kan de officier van justitie bij de rechtbank de vernietiging van de gegevens vorderen. In dat geval wordt een afzonderlijke rechterlijke beslissing gegeven, op grond van artikel 552fa Sv (zie hieronder bij de toelichting op artikel II, onderdeel G).

Artikel II, onderdeel F

Eerste lid

Dit betreft het herstel van een omissie. In artikel 552a Sv wordt belanghebbenden de mogelijkheid geboden zich schriftelijk te beklagen over de inbeslagneming van voorwerpen. De reikwijdte van deze bepaling is uitgebreid naar aanleiding van de opneming van de artikelen over de doorzoeking ter vastlegging van gegevens (artikelen 125i tot en met 125o Sv). Daardoor is onder meer voorzien in de mogelijkheid voor belanghebbenden om zich te beklagen over de vordering medewerking te verlenen aan het ontsleutelen van gegevens op grond van artikel 125k, tweede lid, Sv. Ten onrechte is niet voorzien in de mogelijkheid voor belanghebbenden om zich te beklagen over de vordering tot het verschaffen van toegang tot de aanwezige geautomatiseerde werken of delen daarvan, dan wel het ter beschikking stellen van kennis omtrent de beveiliging op grond van artikel 125k, eerste lid, Sv. Dit artikellid wordt in het eerste lid van dit onderdeel aan artikel 552a, eerste lid, Sv toegevoegd.

Tweede lid

Met de Wet vorderen gegevens financiële sector (Stb. 2004, 109) en de Wet bevoegdheden vorderen gegevens (Stb. 2005, 390) is het toepassingsbereik van artikel 552a Sv verruimd doordat beklag ook mogelijk is over de toepassing van dwangmiddelen in verband met gegevens. Met de Wet computercriminaliteit II is de mogelijkheid voor belanghebbenden opgenomen zich te beklagen over een beslissing van de officier van justitie of van de rechter-commissaris tot ontoegankelijkmaking van gegevens op grond van artikel 125o Sv. Dit betreft een bevoegdheid die kan worden uitgeoefend ten aanzien van gegevens die worden aangetroffen bij de doorzoeking van een geautomatiseerd werk.

Het is van belang dat belanghebbenden zich ook kunnen beklagen over een door de officier van justitie gedane vordering tot het ontoegankelijk maken van gegevens op grond van het voorgestelde artikel 125p Sv. Dit kan de aanbieder betreffen tot wie de vordering is gericht, maar het kan eveneens personen betreffen die de gegevens beschikbaar hebben gesteld voor de verspreiding door middel van het internet. In het tweede lid van het hier toegelichte onderdeel wordt voorgesteld een verwijzing naar artikel 125p Sv toe te voegen aan artikel 552a, eerste lid, Sv. Het beklag kan zich richten op het ontbreken van de noodzaak tot ontoegankelijkmaking om strafbare feiten te beëindigen of te voorkomen. Ook kan het beklag zich erop richten dat het belang van strafvordering zich niet meer verzet tegen de opheffing van de maatregel tot ontoegankelijkmaking zodat de gegevens weer ter beschikking van de beheerder van het geautomatiseerde werk gesteld kunnen worden.

In het voorgestelde artikel 125q Sv is de bevoegdheid van de officier van justitie geregeld tot het opleggen van een dwangsom. Vanwege de nauwe relatie tussen enerzijds de vordering tot ontoegankelijkmaking van gegevens op grond van artikel 125p Sv en anderzijds de opgelegde dwangsom is het aangewezen om voor de rechtsbescherming van de betrokkene aan te sluiten bij de regeling voor het beklag tegen de vordering. Het beklag staat open voor belanghebbenden. Dit is degene tot wie de vordering tot ontoegankelijkmaking van gegevens is gericht. Het beklag is mogelijk zowel tegen de beslissing als zodanig om een dwangsom op te leggen als tegen de modaliteiten daarvan, zoals de hoogte van de dwangsom of de begunstigingstermijn. Het klaagschrift wordt zo spoedig mogelijk na de vordering tot ontoegankelijkmaking van de gegevens ingediend bij de griffie van het gerecht waar de zaak wordt vervolgd (artikel 552a, derde lid, Sv). Indien geen vervolging wordt ingesteld, wordt het klaagschrift zo spoedig mogelijk, maar uiterlijk twee jaar na de vordering tot ontoegankelijkmaking, ingediend bij de griffie van de rechtbank waar de ontoegankelijkmaking is geschied (artikel 552a, vierde lid, Sv). Op de beslissing op het klaagschrift staat beroep in cassatie open (artikel 552d, tweede lid, Sv).

Artikel II, onderdeel G

Artikel 552fa Sv regelt de mogelijkheid voor de officier van justitie om, nadat bij een doorzoeking van een geautomatiseerd werk gegevens zijn aangetroffen en ontoegankelijk gemaakt, de vernietiging van die gegevens te vorderen 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. De vernietiging wordt gelast bij afzonderlijke rechterlijke beschikking, op vordering van de officier van justitie. In dit onderdeel wordt erin voorzien dat als de officier van justitie op grond van het voorgestelde artikel 125p Sv een vordering tot ontoegankelijkmaking van gegevens heeft gericht aan een aanbieder, hij vervolgens de vernietiging van de gegevens kan vorderen die ter uitvoering van de vordering ontoegankelijk zijn gemaakt. Voorwaarde is dat de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. Op grond van artikel 552fa, derde lid, Sv staat voor de officier van justitie beroep in cassatie open tegen een beslissing tot afwijzing van de vordering.

Artikel II, onderdeel H

Dit onderdeel betreft reparatie van artikel 592, tweede lid, Sv. Dit artikel geeft een regeling voor de vergoeding van de kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 126m, 126n, 126nc tot en met 126ni, 126t, 126u, 126uc tot en met

126ui, en 126zja tot en met 126zp Sv. In deze opsomming zijn de artikelen 126na, 126ua, 126zg, 126zh en 126zi Sv ten onrechte niet vermeld. Met de opneming van een verwijzing naar deze artikelen wordt deze omissie hersteld.

De Minister van Justitie,