Raad van State

Kenmerk	W03.12.0306/II
Datum advies	14 september 2012
Vindplaats	Kamerstukken II 2012/2013, 33 662, nr. 4

Volledige tekst

Voorstel van wet tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik camerabeelden en meldplicht datalekken), met memorie van toelichting.

Van dit advies is een samenvatting gemaakt.

Bij Kabinetsmissive van 27 juli 2012, no.12.001757, heeft Uwe Majesteit, op voordracht van de Staatssecretaris van Veiligheid en Justitie, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken, Landbouw en Innovatie, ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik camerabeelden en meldplicht datalekken), met memorie van toelichting.

Het wetsvoorstel strekt ertoe de voorwaarden te verruimen waaronder in de Wet bescherming persoonsgegevens (hierna: Wbp) het gebruik van camerabeelden van strafbare feiten is toegestaan. Daarnaast wordt in de Wbp een geclausuleerde meldplicht datalekken opgenomen die zowel voor de publieke als voor de private sector zal gelden. In de eerste plaats adviseert de Afdeling advisering van de Raad van State het wetsvoorstel te splitsen, gelet op de inhoudelijke verschillen tussen de voorgestelde maatregelen.

Met betrekking tot de voorgestelde verruiming van de mogelijkheden om strafrechtelijke gegevens te verwerken, mist de Afdeling een gedegen probleemanalyse en een toereikende onderbouwing van het nut en de noodzaak van hetgeen daartoe is voorgesteld. Verder stelt de Afdeling vragen over de waarborgen die zullen gelden voor de grootschalige verwerkingen van strafrechtelijke gegevens ten behoeve van derden, nu volgens het voorstel de verplichting van een voorafgaand onderzoek door het College bescherming persoonsgegevens (hierna: Cbp) voor alle soorten verwerkingen (kleinschalig of niet) vervalt. De Afdeling adviseert voorts om in het voorstel dwingend voor te schrijven dat bij een algemene maatregel van bestuur zal worden bepaald dat de verwerking van strafrechtelijke gegevens in de in het voorstel bedoelde zin slechts plaatsvindt met instemming van een bij die maatregel aangewezen bestuursorgaan of een andere autoriteit.

Wat de meldplicht datalekken betreft adviseert de Afdeling de voorgestelde regeling van de meldplicht nader te specificeren. De voorgestelde bepaling is onbepaald. Daardoor is niet duidelijk welke gevallen er wel of niet onder vallen. Nu de bepaling door straf wordt gehandhaafd, staat zij door haar onbepaaldheid op gespannen voet met het rechtszekerheidsbeginsel. Verder is voor betrokkenen niet voorzienbaar wanneer van een overtreding sprake is. De Afdeling stelt daarom ook vraagtekens bij de effectiviteit van de meldplicht en bij de lasten die deze meebrengt. De reikwijdte van de meldplicht is naar het oordeel van de Afdeling ook onduidelijk, omdat niet vaststaat in welke gevallen van een inbreuk op beveiligingsmaatregelen kan worden gesproken. Ten slotte maakt de Afdeling een opmerking over de schorsende werking van het beroep en het verzet tegen de invordering van een bestuurlijke boete wegens overtreding van de meldplicht.

Gelet op de vraagtekens die worden gezet bij de probleemanalyse en onderbouwing van nut en noodzaak van de verruiming van het gebruik van camerabeelden van strafbare feiten alsmede gelet op de onbepaaldheid van de door straf te handhaven meldplicht bij datalekken, is de Afdeling van oordeel dat het wetsvoorstel deels nader dient te worden overwogen.

1. Splitsing

In het wetsvoorstel worden twee maatregelen voorgesteld. Ten eerste wordt de mogelijkheid tot het gebruik door particulieren van camerabeelden die betrekking hebben op strafbare feiten, verruimd. Daaronder valt het plaatsen van deze beelden op internet. Ten tweede wordt een meldplicht in geval van datalekken voorgesteld. Beide voorstellen zijn gezamenlijk in het onderhavige voorstel opgenomen. Volgens de toelichting is deze keuze gerechtvaardigd uit een oogpunt van wetgevingseconomie en vanwege het inhoudelijke verband tussen beide voorgestelde maatregelen. Zichtbaarheid is hierbij het kernbegrip: "Cameratoezicht bevordert het zichtbaar maken van criminaliteit en overlast in de fysieke wereld, waardoor een meer effectieve bestrijding van deze verschijnselen mogelijk wordt. De meldplicht datalekken bevordert het zichtbaar worden van de consequenties voor burgers van computercriminaliteit of vormen van verwijtbare nalatigheid bij de beveiliging van gegevens in de digitale wereld." (*zie noot* 1) Deze redenering acht de Afdeling niet overtuigend. Beide onderdelen van het onderhavige voorstel strekken weliswaar tot wijziging van de Wbp; zij betreffen echter verschillende onderwerpen die inhoudelijk weinig samenhang vertonen. De Afdeling adviseert daarom het wetsvoorstel te splitsen. Daarmee kan ook worden voorkomen dat door mogelijke bezwaren in de verdere wetgevingsprocedure tegen één van beide onderdelen, beide regelingen vertraging zullen oplopen.

2. Verruiming gebruik camerabeelden strafbare feiten

Het voorstel stelt het voorafgaand onderzoek door het Cbp (*zie noot* 2) niet meer verplicht in geval van de voorgenomen verwerking van strafrechtelijke gegevens op grond van artikel 22, vierde lid onder c, van de Wbp. (*zie noot* 3) Het vereiste van voorafgaand onderzoek door het Cbp wordt vervangen door het vereiste van een voorafgaande toestemming van de officier van justitie, zo stelt de toelichting. Dit wordt bepaald in een algemene maatregel van bestuur.

a. Nut en noodzaak

De Afdeling onderkent dat camerabeelden van strafbare feiten een nuttig hulpmiddel kunnen zijn bij de opsporing van strafbare feiten en ook dat "hoe sneller de beelden bij politie en justitie beschikbaar zijn, hoe groter de kans (is) op een succesvolle opsporing van het strafbare feit". (*zie noot* 4) De toelichting gaat niet specifiek in op de aard en de omvang van het probleem dat het onderhavige voorstel beoogt op te lossen. Hierdoor blijft onduidelijk waarom de nieuwe mogelijkheid van de verwerking van bijzondere persoonsgegevens die

het voorstel beoogt te creëren, noodzakelijk is. De Afdeling wijst erop dat - behoudens het geval van ondubbelzinnige toestemming - op grond van artikel 8 Wbp (*zie noot* 5) iedere verwerking moet voldoen aan de algemene voorwaarde van de noodzakelijkheid.
De toelichting stelt dat het beeldmateriaal van strafbare feiten in ruime mate beschikbaar is en dat burgers en bedrijven graag bereid zijn om dat beeldmateriaal beschikbaar te stellen. (*zie noot* 6) De huidige Aanwijzing opsporingsberichtgeving (*zie noot* 7) bevat richtlijnen voor het openbaar ministerie ten aanzien van de wijze waarop het materiaal waarover het beschikt, onder de aandacht van het publiek kunnen worden gebracht. Daaronder vallen ook camerabeelden van strafbare feiten. In de toelichting wordt niet ingegaan op de vraag of zich problemen voordoen met betrekking tot de wijze waarop het openbaar ministerie met deze beelden omgaat. Volstaan wordt met de opmerking dat het wetsvoorstel niet bedoeld is om afbreuk te doen aan de bestaande praktijk. Het is de bedoeling om deze praktijk aan te vullen "voor de gevallen waarin de inspanningen van politie en justitie alleen misschien niet het meest optimale resultaat kunnen bereiken." (*zie noot* 8) In welke gevallen de inspanningen van politie en justitie "misschien" niet tot "het meest optimale resultaat" leiden en hoe vaak die zich voordoen, wordt niet toegelicht. Wel wordt gesteld dat het "niet ondenkbaar is" dat "in een individueel geval bij een gerichte inspanning van een burger in de eigen omgeving en de context die hij zelf het beste kent, meer informatie over een strafbaar feit naar voren kan komen dan wanneer dit achterwege wordt gelaten". Dit is naar het oordeel van de Afdeling ontoereikend als motivering voor de voorgestelde versoepeling van het regime uit de Wbp. Dit geldt te meer, daar het hier om persoonsgegevens gaat waarvan de verwerking een aanzienlijke inbreuk maakt op de privacy van betrokkenen, zoals slachtoffers en omstanders bij strafbare feiten alsmede onterecht verdachte personen. Uitgangspunt is dat de verwerking van dergelijke gegevens verboden is. (*zie noot* 9) Verder wijst de Afdeling erop dat burgers ook in de eigen omgeving en vanuit de context die zij het beste kennen, kunnen verwijzen naar de berichtgeving van het openbaar ministerie, bijvoorbeeld via sociale media.

De Afdeling vestigt in dit verband ook de aandacht op het advies van het College van procureurs-generaal. (*zie noot* 10) Daaruit blijkt dat eerder een probleem bestaat met betrekking tot de vraag hoe bepaalde camerabeelden zo snel mogelijk en zonder onnodige belemmeringen door de politie kunnen worden gebruikt in de opsporing. Het College stelt voor een bevoegdheid voor de politie op te nemen tot het vormvrij vorderen van opgeslagen camerabeelden en daartoe artikel 126nd Wetboek van Strafvordering aan te passen. In reactie hierop wordt in de toelichting louter gesteld dat de uitwerking hiervan een afzonderlijke afweging vereist "die niet in de context van dit wetsvoorstel kan plaatsvinden". (*zie noot* 11) De Afdeling is evenwel van oordeel dat het door het College gesignaleerde probleem bij de vordering van beeldmateriaal ten minste meegenomen dient te worden in een deugdelijke probleemanalyse uitmondend in een dragende motivering van de noodzaak van hetgeen is voorgesteld. Deze ontbreekt vooralsnog.

De Afdeling adviseert een inzichtelijke probleemanalyse in de toelichting op te nemen en de noodzaak van de voorgestelde uitbreiding van de mogelijkheid om strafrechtelijke gegevens ten behoeve van derden te verwerken, dragend te motiveren.

b. Reikwijdte voorstel, wettelijk kader
De toelichting merkt over de reikwijdte van het voorstel op dat het voorstel beperkt blijft tot het aan derden - door middel van het plaatsen op internet - verstrekken van beelden die zelf rechtmatig worden verwerkt op grond van artikel 22, tweede lid, onder b, van de Wbp. Volgens de toelichting moet het dus gaan om een verwerking voor de bescherming van het eigen belang van de verantwoordelijke tegen het gevaar dat uitgaat van strafbare feiten. Daarbij wordt opgemerkt dat het voorstel niet ziet op de verwerking van camerabeelden van

andere aard dan camerabeelden die afkomstig zijn van geïnstalleerde bewakingscamera's. Dit betekent dat de verwerking van camerabeelden van strafbare feiten die bijvoorbeeld vervaardigd zijn met mobiele telefoons door toevallige passanten, niet onder de reikwijdte van het voorstel valt, aldus de toelichting. (*zie noot* 12)
De Afdeling acht deze redenering onduidelijk en merkt daarbij op dat het huidige artikel 22, vierde lid, van de Wbp betrekking heeft op de verwerking van strafrechtelijke gegevens ten behoeve van derden. Blijkens de memorie van toelichting bij de huidige Wbp dient deze bepaling ter bescherming van de belangen van derden die het slachtoffer zouden kunnen worden van criminaliteit. (*zie noot* 13) Begrijpt de Afdeling de toelichting goed, dan is het niet de bedoeling van de voorgestelde wijzigingen om de derde te beschermen. Het zou juist gaan om de bescherming van "het eigen belang van de verantwoordelijke tegen het gevaar dat uitgaat van strafbare feiten" en om het bieden van ruimte "aan particulieren om ter beveiliging van hun rechtmatige belangen strafrechtelijke gegevens te verwerken". (*zie noot* 14) Het tonen van beelden van strafbare feiten op internet zou dan behulpzaam kunnen zijn bij de opsporing van strafbare feiten die jegens de verantwoordelijke zelf zijn gepleegd of jegens personen die bij hem in dienst zijn. Daarvoor wordt een koppeling gelegd tussen het vierde lid, onderdeel c en het tweede lid, onderdeel b van artikel 22 Wbp. De Afdeling merkt echter op dat de tekst van het wetsvoorstel de beperking van de reikwijdte van het voorstel tot de gevallen genoemd in artikel 22, tweede lid, onder b, van de Wbp niet regelt. Ook kan uit het huidige vierde lid onder c, van artikel 22 niet worden afgeleid dat de daarin bedoelde verwerking slechts betrekking heeft op verwerking van camerabeelden die afkomstig zijn van geïnstalleerde bewakingscamera's en niet ook op camerabeelden die bijvoorbeeld vervaardigd zijn met mobiele telefoons door toevallige passanten.

De Afdeling adviseert de reikwijdte van het voorstel te verduidelijken en daarbij de toelichting en de tekst van het wetsvoorstel met elkaar in overeenstemming te brengen. Tevens adviseert de Afdeling uiteen te zetten welk juridisch kader geldt voor het gebruik van camerabeelden ten behoeve van derden, wanneer deze beelden vervaardigd zijn met bijvoorbeeld mobiele telefoons door toevallige passanten.

c. Voorafgaand onderzoek van het Cbp bij grootschalige verwerkingen
Uit de toelichting blijkt dat er voor gekozen is om de verplichting van voorafgaand onderzoek door het Cbp los te laten, omdat een dergelijk onderzoek omslachtig en langdurig is. (*zie noot* 15) Dit zou te maken hebben met het feit dat de procedure van voorafgaand onderzoek "niet [is] toegesneden op de beoordelingen van zeer kleinschalige verwerkingen als de beoordeling van camerabeelden die doorgaans niet meer dan één of enkele minuten aan relevant materiaal bieden, maar op verwerkingen met een permanent of anderszins langduriger of grootschaliger karakter." (*zie noot* 16) De Afdeling wijst erop dat in het voorstel geen onderscheid is gemaakt tussen grootschalige en kleinschalige verwerking van strafrechtelijke gegevens ten behoeve van derden. Als gevolg hiervan zal de eis van een voorafgaand onderzoek door het Cbp strikt genomen ook niet meer gelden voor verwerkingen met "een permanent of anderszins langduriger of grootschaliger karakter" die plaatsvinden op grond van artikel 22, vierde lid, onder c. Het is niet duidelijk waarom de eis van voorafgaand onderzoek voor deze verwerkingen vervalt. Het gaat hier immers niet om situaties met spoedeisend belang, waarin behoefte bestaat aan een snelle reactie van het Cbp. Gelet op de privacybelangen van de betrokkenen, die bij die verwerkingen extra zwaar zullen wegen, is het laten vervallen van de eis van voorafgaand onderzoek door het Cbp naar het oordeel van de Afdeling onwenselijk.

De Afdeling adviseert in de toelichting aan te geven welke waarborgen zullen gelden ten aanzien van verwerkingen van strafrechtelijke gegevens op grond van artikel 22, vierde lid,

onder c met "een permanent of anderszins langduriger of grootschaliger karakter" en het voorstel aan te passen.

d. Toestemming van de officier van justitie als absolute verplichting

In de toelichting wordt gesproken van de toestemming van de officier van justitie als een absolute eis die voorafgaat aan de plaatsing van de beelden op internet door particulieren. Zonder deze toestemming zou een dergelijke verwerking van strafrechtelijke gegevens onrechtmatig zijn vanwege strijd met de Wbp. De Afdeling constateert dat de tekst van het voorstel hiermee niet in overeenstemming is; hierin wordt slechts bepaald dat in een algemene maatregel van bestuur bepaald kan worden dat een dergelijke toestemming is vereist. (*zie noot* 17)

De Afdeling adviseert in het voorgestelde artikel 22, zevende lid, van de Wbp de woorden "kan worden bepaald" te vervangen door "wordt bepaald".

3. Meldplicht datalekken

In het wetsvoorstel wordt een meldplicht datalekken voorgesteld voor het geval er inbreuk is gemaakt op de beveiligingsmaatregelen die door de verantwoordelijke zijn genomen. De meldplicht zal zowel voor de publieke als voor de private sector gelden.

a. Onbepaaldheid meldplicht

De Europese Commissie heeft op 25 januari 2012 een voorstel gepresenteerd voor een Algemene verordening gegevensbescherming (hierna: conceptverordening). (*zie noot* 18) Daarin is ook een meldplicht datalekken opgenomen. De hier voorgestelde meldplicht is, in tegenstelling tot de in de conceptverordening opgenomen meldplicht, niet algemeen. Zij is geclausuleerd en geldt alleen wanneer de inbreuk op de beveiliging zodanig is, dat "redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op nadelige gevolgen voor de bescherming van persoonsgegevens" die door de verantwoordelijke worden verwerkt. (*zie noot* 19) Met deze clausulering is beoogd te voorkomen dat elk denkbaar datalek moet worden gemeld, hetgeen afbreuk kan doen aan de effectiviteit van de meldplicht. Bovendien leidt een meldplicht zonder enige beperking tot een nodeloze belasting van bedrijfsleven en overheid, aldus de toelichting. (*zie noot* 20)

Hoewel de Afdeling begrip heeft voor de wenselijkheid van enige clausulering, wijst zij erop dat de gekozen formulering onbepaald is. Begrippen als 'redelijkerwijs', 'aanmerkelijk' en 'nadelig' kunnen verschillend worden ingevuld door het Cbp en degene die als verantwoordelijke in de zin van de Wbp kan worden aangemerkt. Onduidelijk is hierdoor op welke gevallen de bepaling wel of niet ziet. Voorts is het naar het oordeel van de Afdeling niet de taak van het Cbp om een door straf te handhaven bepaling als deze via beleidsregels nader te preciseren, zoals de toelichting suggereert. (*zie noot* 21) Dit is aan de wetgever.

Nu de voorgestelde meldplicht een bepaling betreft die met een straf (bestuurlijke boete) is bedreigd, is het strafrechtelijke lex certa beginsel in het geding. (*zie noot* 22) Dit beginsel vereist dat de delictsomschrijving van een strafbepaling zo precies en zo beperkt mogelijk is. Voor de burger moet voorzienbaar zijn welke concrete handelingen (of het nalaten ervan) tot straffen kunnen leiden. De onbepaaldheid van de thans voorgestelde bepaling brengt mee dat zij op gespannen voet komt te staan met het rechtszekerheidsbeginsel en voorts dat van voorzienbaarheid, zoals hiervoor uitgelegd, niet gesproken kan worden.

Onverminderd het voorgaande wijst de Afdeling erop dat de voorgestelde vage omschrijving van de meldplicht in de praktijk tot het omgekeerde resultaat kan leiden. Met de voorgestelde clausulering is volgens de toelichting, zoals hierboven gesteld, beoogd te voorkomen dat de effectiviteit van de meldplicht aan betekenis zal verliezen als elk denkbaar

datalek in aanmerking komt om te worden gemeld. (*zie noot* 23) Ondanks deze clausulering worden nog altijd 66.000 meldingen per jaar verwacht, zo blijkt uit de toelichting. (*zie noot* 24) De Afdeling wijst erop dat juist de vaagheid van de norm en de forse boete die op het niet naleven van de meldplicht staat, ertoe kunnen leiden dat vaker onnodig zal worden gemeld met alle gevolgen van dien voor de effectiviteit van de melding en de hoogte van bestuurlijke en administratieve lasten.
De Afdeling adviseert de voorgestelde meldplichtbepaling nader te preciseren en het voorstel daartoe aan te passen.

b. Reikwijdte meldplicht en definitie datalek
De voorgestelde meldplicht geldt alleen wanneer sprake is van een inbreuk op de beveiligingsmaatregelen als bedoeld in artikel 13 van de Wbp. In dit artikel is een verplichting neergelegd voor de verantwoordelijke tot het nemen van passende technische en organisatorische maatregelen teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Ten eerste wijst de Afdeling op de mogelijkheid dat de verantwoordelijke in het geheel geen maatregelen heeft genomen ter beveiliging van de persoonsgegevens of dat deze maatregelen niet als passend zijn aan te merken. De voorgestelde meldplicht zou in deze situatie niet gelden, omdat strikt genomen niet gesproken kan worden van een inbreuk op de beveiligingsmaatregelen van artikel 13 van de Wbp.
De Afdeling adviseert in de toelichting aan dit aspect aandacht te besteden en de tekst van de voorgestelde bepaling zo nodig aan te passen.

Ten tweede merkt de Afdeling op dat in de toelichting verschillende situaties worden genoemd die aanleiding kunnen geven tot het ontstaan van een meldplicht. Gewezen wordt op het slordig omgaan met het beheer van wachtwoorden, een inbraak, waterschade of blikseminslag, maar ook het verlies van een mobiele telefoon, de diefstal van een laptop of het zoekraken van een geheugenstick. (*zie noot* 25) In het verlengde hiervan zou gedacht kunnen worden aan het verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat en het als oud papier aanbieden van gevoelige stukken. Hoewel hier sprake is van verlies van gegevens, kan strikt genomen niet gesteld worden dat dit verlies steeds het gevolg is van een inbreuk op de beveiliging.
De Afdeling adviseert in te gaan op de relatie tussen de meldplicht en de vereiste inbreuk op de beveiligingsmaatregelen en daarbij nader toe te lichten in welke gevallen sprake is van een inbreuk op de beveiliging.

c. Boetebevoegdheid van het Cbp: schorsende werking
Indien het geconstateerde datalek ten onrechte niet bij het Cbp wordt gemeld, kan het Cbp op grond van het voorstel een bestuurlijke boete opleggen tot een maximaal bedrag van 450.000 euro. (*zie noot* 26) Dezelfde maximale boete kan door het Cbp worden opgelegd wegens het niet nakomen van de meldplicht die thans voor telecombedrijven geldt op grond van artikel 11.3a van de Telecommunicatiewet. (*zie noot* 27)

De Afdeling wijst erop dat in artikel 15.12 van de Telecommunicatiewet is voorzien in de schorsende werking van het beroep tegen boetebesluiten en in artikel 15.14 in de schorsende werking van verzet tegen een dwangbevel tot invordering van de bestuurlijke boete. (*zie noot* 28) Het voorstel wijzigt artikel 15.12 niet. De Afdeling gaat er daarom van uit dat voor het instellen van beroep door telecombedrijven tegen boetebesluiten de schorsende werking blijft bestaan.
Het voorstel beoogt wel artikel 15.14 te wijzigen, waardoor verzet gedaan door

telecombedrijven tegen een dwangbevel tot invordering van de bestuurlijke boete niet langer de schorsende werking zal hebben. Volgens de toelichting is hiervoor gekozen in verband met de toedeling van de boetebevoegdheid aan het Cbp. Daarbij "dient te worden uitgesloten dat de schorsende werking van het verzet wel zou bestaan bij besluiten van het Cbp genomen op grond van de Tw, terwijl deze niet bestaat bij bestuurlijke boetes opgelegd op grond van de Wbp," zo luidt de toelichting. (*zie noot* 29)
De Afdeling is van oordeel dat het verplaatsen van de boetebevoegdheid van OPTA naar het Cbp, waardoor voor telecombedrijven het rechtsbeschermingsregime uit de Wbp van toepassing zal zijn, niet als een inhoudelijk argument kan dienen voor het ontzeggen van de schorsende werking aan verzet tegen een dwangbevel tot invordering van de bestuurlijke boete. De Afdeling ziet niet in waarom deze voorgestelde wijziging noodzakelijk zou zijn.

Daarnaast wijst de Afdeling erop dat de voorgestelde algemene meldplicht in de Wbp grotendeels overeenkomt met de meldplicht die thans geldt voor telecombedrijven op grond van artikel 11.3a van de Telecommunicatiewet. Het maximale boetebedrag voor het niet nakomen van beide meldplichten is ook hetzelfde, namelijk 450.000 euro. Gelet hierop verdient het naar het oordeel van de Afdeling aanbeveling om ook voor het niet nakomen van de algemene meldplicht op grond van de Wbp te voorzien in de schorsende werking van het beroep en van het verzet tegen een dwangbevel tot invordering van de bestuurlijke boete. De Wbp voorziet thans slechts in de schorsende werking van bezwaar tegen boetebesluiten. (*zie noot* 30)

De Afdeling adviseert de schorsende werking van verzet tegen een dwangbevel tot invordering van de bestuurlijke boete in de Telecommunicatiewet te handhaven. Tevens geeft de Afdeling in overweging de regeling omtrent de schorsende werking van beroep en van verzet tegen een dwangbevel tot invordering van de bestuurlijke boete, zoals opgenomen in de Telecommunicatiewet, ook op te nemen ten aanzien van de voorgestelde algemene meldplicht op grond van de Wbp.

4. Voor redactionele kanttekeningen verwijst de Afdeling naar de bij het advies behorende bijlage.

De Afdeling advisering van de Raad van State geeft U in overweging het voorstel van wet niet te zenden aan de Tweede Kamer der Staten-Generaal dan nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State

Bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no.W03.12.0306/II met redactionele kanttekeningen die de Afdeling in overweging geeft.

- In artikel I, onderdeel C, uitgaan van de tekst van artikel 31, eerste lid, onderdeel c, van de Wbp, zoals gewijzigd bij wet van 26 januari 2012 (Stb. 2012, nr. 33).
- In het voorgestelde artikel 34a, eerste lid, van de Wbp "aanmerkelijk risico op" vervangen door: aanmerkelijke kans op.
- In het wetsvoorstel kiezen voor één begrip met betrekking tot beveiligingsmaatregelen van artikel 13 van de Wbp en dit begrip consequent gebruiken. Zie de voorgestelde wijzigingen in artikelen: 14 ("de maatregelen, bedoeld in artikel 13" en "de beveiligingsmaatregelen, bedoeld

in artikel 13") en artikel 34a ("de beveiliging, bedoeld in artikel 13").
- In het voorgestelde zevende lid van artikel 22 van de Wbp "bestuursorgaan" vervangen door: bestuursorgaan.
- In het voorgestelde artikel I, onderdeel B, "2. Het zevende lid komt te luiden: 7." vervangen door: 2. Het achtste lid komt te luiden: 8.

Nader rapport (reactie op het advies) van 12 juni 2013

1. Splitsing

In het wetsvoorstel dat bij de Afdeling advisering van de Raad van State aanhangig is gemaakt werden twee maatregelen voorgesteld. Ten eerste werd voorgesteld de mogelijkheid tot het gebruik door particulieren van camerabeelden die betrekking hebben op strafbare feiten, te verruimen. Ten tweede werd een meldplicht in geval van datalekken voorgesteld. Beide voorstellen waren gezamenlijk in het wetsvoorstel opgenomen. Volgens de toelichting was deze keuze gerechtvaardigd uit een oogpunt van wetgevingseconomie en vanwege het inhoudelijke verband tussen beide voorgestelde maatregelen. De Afdeling acht het inhoudelijke verband niet overtuigend. Beide onderdelen van het onderhavige voorstel strekken weliswaar tot wijziging van de Wet bescherming persoonsgegevens (hierna: Wbp); zij betreffen echter verschillende onderwerpen die inhoudelijk weinig samenhang vertonen. De Afdeling adviseert daarom het wetsvoorstel te splitsen. Dit advies is gevolgd. Het onderhavige wetsvoorstel bevat alleen de invoering van een meldplicht datalekken. In dit nader rapport wordt daarom alleen ingegaan op de door de Afdeling gemaakte opmerkingen over de meldplicht datalekken (paragrafen 1, 3 en 4). De maatregel die ziet op verruiming van het gebruik door particulieren van camerabeelden die betrekking hebben op strafbare feiten, zal op termijn in een afzonderlijk wetsvoorstel worden ondergebracht.

Een splitsing over twee voorstellen heeft niet alleen het voordeel dat kan worden voorkomen dat door mogelijke bezwaren in de verdere wetgevingsprocedure tegen één van beide onderdelen, beide onderdelen vertraging zullen oplopen, maar ook dat een nadere prioritering van de te realiseren voornemens kan worden bewerkstelligd. Dit is om twee redenen van belang. Ten eerste in verband met het in het regeerakkoord van het kabinet-Rutte II van 29 oktober 2012 aangekondigde voornemen om te komen tot uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens (hierna: het Cbp) om bestuurlijke boetes op te leggen (vgl. ook de motie van het lid Recourt, Kamerstukken II 2011/12, 32761, nr. 22). De Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken zullen bij nota van wijziging op het onderhavige wetsvoorstel voorzien in een regeling die strekt tot uitbreiding van de bestuurlijke boetebevoegdheden van het Cbp met het oog op de versterking van de handhaving van de Wbp. Gelet op het ingrijpende karakter van deze nota van wijziging zal over ontwerp van deze nota van wijziging het advies van de Afdeling advisering van de Raad van State worden gevraagd. Ten tweede zullen de nationale wetgevingsinspanningen op het gebied van de Wet bescherming persoonsgegevens moeten worden afgewogen en beoordeeld in het licht van de wetgevingsinspanningen die sedert januari 2012 worden verricht ten behoeve van de herziening van de Europese regelgeving inzake verwerking en bescherming van persoonsgegevens (totstandkoming algemene verordening gegevensbescherming alsmede een richtlijn voor gegevensbescherming bij

opsporing en vervolging).
De splitsing van het wetsvoorstel is aanleiding geweest voor een herschikking van de memorie van toelichting; een aantal paragrafen uit het algemene gedeelte van de toelichting over de meldplichtbepaling is overgeheveld naar het artikelsgewijze gedeelte.

3. Meldplicht datalekken

Wat de meldplicht datalekken betreft adviseert de Afdeling de voorgestelde regeling van de meldplicht nader te specificeren. De voorgestelde bepaling is onbepaald. Daardoor is niet duidelijk welke gevallen er wel of niet onder vallen. Nu de bepaling door straf wordt gehandhaafd, staat zij door haar onbepaaldheid op gespannen voet met het rechtszekerheidsbeginsel. Verder is voor betrokkenen niet voorzienbaar wanneer van een overtreding sprake is. De Afdeling stelt daarom ook vraagtekens bij de effectiviteit van de meldplicht en bij de lasten die deze meebrengt. De reikwijdte van de meldplicht is naar het oordeel van de Afdeling ook onduidelijk, omdat niet vaststaat in welke gevallen van een inbreuk op beveiligingsmaatregelen kan worden gesproken. Ten slotte maakt de Afdeling een opmerking over de schorsende werking van het beroep en het verzet tegen de invordering van een bestuurlijke boete wegens overtreding van de meldplicht.

a. Onbepaaldheid meldplicht

De Afdeling vergelijkt de in dit wetsvoorstel voorgestelde –nationale– meldplicht met de door de Europese Commissie voorgestelde meldplicht in artikel 31 van het voorstel van een Algemene verordening gegevensbescherming (hierna: conceptverordening). Hoewel de nationale meldplicht voor datalekken qua reikwijdte aansluit bij de meldplicht datalekken in de conceptverordening (er is sprake van een brede meldplicht, in tegenstelling tot de specifieke meldplicht in artikel 11.3a van de Telecommunicatiewet), is deze minder verstrekkend omdat de nationale meldplicht een clausulering bevat waarmee wordt beoogd bagatelzaken van de meldplicht uit te sluiten. De conceptverordening kent een dergelijke clausulering niet waardoor elk denkbaar datalek aan de toezichthouder zou moeten worden gemeld.
Hoewel de Afdeling begrip heeft voor de wenselijkheid van enige clausulering, wijst zij erop dat de gekozen formulering onbepaald is. Ik meen dat de gekozen formulering aansluit bij de normstelling in de Wbp, die naar zijn aard nu eenmaal als algemeen-abstract kan worden gekenschetst, hetgeen kan worden verklaard door de grote diversiteit aan verwerkingen van persoonsgegevens in de private en publieke sector. Ik meen dat de gekozen formulering voldoende duidelijk is en in de praktijk ook goed hanteerbaar; een nadere precisering zou ontegenzeggelijk leiden tot een beperktere meldplicht dan wenselijk is. Daarbij wijs ik erop, dat in paragraaf 3.2.2 van de memorie van toelichting een "beslismodel" is uitgeschreven met behulp waarvan een voor de verwerking van persoonsgegevens verantwoordelijke die met een datalek wordt geconfronteerd, kan beoordelen of dit valt onder de voorgestelde wettelijke meldplicht van artikel 34a Wbp. Ik neem daarbij in aanmerking dat van een verantwoordelijke een redelijke inspanning mag worden gevraagd om, zo nodig met behulp van deskundig advies, het eigen handelen op een wettelijke norm af te stemmen (vlg. EHRM 28 juni 2011, LJN BT2901 (Financiële Dagblad B.V./Nederland), EHRM 15 november 1996, nr. 17862/91 (Cantoni/Frankrijk) en 25 juni 2009, nr. 12157/05 (Liivik/Estland). Daarnaast ga ik ervan uit dat ook het Cbp, door het vaststellen van richtsnoeren, de praktijk enig houvast kan geven. Ik meen dat op deze wijze in voldoende mate voor de verantwoordelijke voorzienbaar zal zijn in welke concrete gevallen het nalaten van het doen van een melding van een datalek tot een bestuurlijke boete door het Cbp aanleiding kan geven. In mijn optiek kan de voorgestelde meldplicht als een administratiefrechtelijke verplichting worden aangemerkt en is van een spanning met het rechtszekerheidsbeginsel geen sprake.

Naar aanleiding van de opmerking van de Afdeling dat het niet de taak is van het Cbp om een

door straf te handhaven bepaling door middel van "beleidsregels" nader te preciseren, merk ik op dat mij dit ook niet voor ogen staat. Om beter tot uitdrukking te brengen wat wel van het Cbp mag worden verwacht, heb ik het in de memorie van toelichting gebruikte begrip "boetebeleidsregels" vervangen door het begrip "richtsnoeren" (paragraaf 3.2). Richtsnoeren zijn voor het Cbp een middel om bij te dragen aan verduidelijking van de wettelijke normen. Helderheid over toepasselijke normen bevordert de naleving ervan en komt ook het toezicht door het Cbp ten goede. Het vaststellen van richtsnoeren laat uiteraard de handhavende taak van het Cbp onverlet. Het Cbp kan met het vaststellen van richtsnoeren, o.a. door middel van voorbeelden, de praktijk houvast bieden in welke gevallen wel en niet behoeft te worden gemeld.
De Afdeling stelt daarnaast vraagtekens bij de effectiviteit van de meldplicht en bij de lasten die deze meebrengt. De onbepaaldheid van de meldplicht in combinatie met de forse boete die op het niet naleven staat, zou ertoe kunnen leiden dat vaker onnodig zal worden gemeld met alle gevolgen van dien. Uit het voorgaande moge blijken dat ik de kritiek van de Afdeling op de onbepaaldheid niet deel. In mijn optiek is de meldplicht voldoende duidelijk geformuleerd en is de clausulering waarmee bagatelzaken van de meldplicht worden uitgezonderd, essentieel om ervaring op te doen met een brede meldplicht als deze. Daarnaast meen ik dat de noodzaak om meldingen van datalekken te doen vooral ook zal afhangen van de naleving van verplichting om zorg te dragen voor een adequate beveiliging van persoonsgegevens, zodat deze niet worden blootgesteld aan onrechtmatige verwerking of verlies. Het Cbp heeft in februari 2013 richtsnoeren gepubliceerd waarin het aangeeft wat het van de beveiliging van persoonsgegevens verwacht (www.cbpweb.nl). Het valt moeilijk te voorspellen wat de effecten hiervan zijn, maar in zijn algemeenheid mag worden verwacht dat deze richtsnoeren eraan bijdragen dat de verantwoordelijken investeren in een goede en op de specifieke kenmerken en risico's van de verwerking van toegesneden beveiliging, zodat het lekken van persoonsgegevens wordt voorkomen of beperkt.

Alles afwegend heb ik in de opmerkingen van de Afdeling geen aanleiding gezien de voorgestelde meldplichtbepaling nader te preciseren. Wel heb ik in de memorie van toelichting de reikwijdte van de voorgestelde meldplichtbepaling verduidelijkt.

b. Reikwijdte meldplicht en definitie datalek

Ingevolge artikel 13 van de Wbp dient de voor de verwerking van de persoonsgegevens verantwoordelijke (private of publieke) instantie passende technische en organisatorische maatregelen te nemen teneinde de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De Afdeling wijst in de eerste plaats op de mogelijkheid dat de verantwoordelijke in het geheel geen maatregelen heeft genomen ter beveiliging van de persoonsgegevens of dat deze maatregelen niet als passend zijn aan te merken. De voorgestelde meldplicht zou in deze situatie niet gelden, omdat strikt genomen niet gesproken kan worden van een inbreuk op de beveiligingsmaatregelen van artikel 13 van de Wbp.

Hoewel de redenering van de Afdeling strikt genomen juist is, zie ik geen noodzaak om de voorgestelde bepaling aan te passen omdat het een in hoge mate hypothetische situatie betreft. Indien een verantwoordelijke wordt geconfronteerd met een datalek waarbij persoonsgegevens op straat zijn komen te liggen, zal hij zich niet snel verweren door te stellen dat hij het datalek niet behoeft te melden omdat hij in het geheel geen beveiligingsmaatregelen heeft getroffen. Daarmee beschadigt hij zijn eigen reputatie en maakt hij zich kwetsbaar voor schadeclaims. Het is in mijn optiek dan ook logisch om bij de omschrijving van de meldplicht het verband met de beveiligingsplicht te leggen. Daarmee beoogt de wetgever de verantwoordelijke aan te zetten om te investeren in een goede

beveiliging, zodat datalekken zoveel mogelijk worden voorkomen of beperkt.
In de tweede plaats wijst de Afdeling erop dat in de toelichting verschillende situaties worden genoemd die aanleiding kunnen geven tot het ontstaan van een meldplicht. De Afdeling meent dat strikt genomen niet kan worden gesteld dat het verlies van persoonsgegevens in de genoemde situaties steeds het gevolg is van een inbreuk op de beveiliging. Naar het mij voorkomt, gaat de Afdeling uit van een te beperkte uitleg van het inbreukvereiste. Ter verduidelijking merk ik op dat niet noodzakelijkerwijs sprake behoeft te zijn van tekortschietende beveiligingsmaatregelen. Van een inbreuk op de beveiligingsmaatregelen kan ook sprake zijn indien de beveiliging van voldoende niveau is, maar de beveiligingsmaatregelen worden teniet gedaan of omzeild. Denk bijvoorbeeld aan een hack van een ICT-systeem dat persoonsgegevens bevat of de diefstal van een laptop of mobiele telefoon uit een afgesloten locker. Er zijn echter ook situaties denkbaar waarin de inbreuk op de beveiligingsmaatregelen het gevolg is van een tekortschietende beveiliging, die de verantwoordelijke zelf kan worden aangerekend. Dit kan variëren van een niet adequate en vakkundig toegepaste beveiliging van de bestanden of de gegevens, tot menselijke fouten van ondergeschikten. Denk bijvoorbeeld aan het slordig omgaan met het beheer van wachtwoorden die toegang geven tot informatiebestanden of aan de door de Afdeling genoemde situaties van het per ongeluk verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat en het als oud papier aanbieden van gevoelige stukken. De door de Afdeling genoemde situaties zijn vergelijkbaar met het zoekraken van een mobiele telefoon of een geheugenstick. In al deze situaties wordt het verlies van persoonsgegevens en de blootstelling aan risico's van ongeoorloofde toegang of onrechtmatige verwerking ervan, veroorzaakt door een inbreuk op de beveiligingsmaatregelen. Ik heb in paragraaf 3.1 van de memorie van toelichting nader toegelicht in welke gevallen van een inbreuk op de beveiliging kan worden gesproken. In die paragraaf wordt ook vermeld dat de meldplicht alleen dan niet geldt wanneer voorzieningen van algemene aard die niet specifiek zijn gericht op de beveiliging van persoonsgegevens worden aangetast. Als bijvoorbeeld een blikseminslag tot gevolg heeft dat het bedrijfspand afbrandt, waarbij ook persoonsgegevens verloren gaan, zal niet van een inbreuk op de beveiligingsmaatregelen kunnen worden gesproken.

c. **Boetebevoegdheid van het Cbp; schorsende werking**

Zoals in de paragrafen 4 en 6 van het algemeen gedeelte van de memorie van toelichting is aangegeven is ervoor gekozen, de meldplicht op grond van artikel 11.3a van de Telecommunicatiewet bij het Cbp te beleggen, het Cbp te belasten met het toezicht en de handhaving van deze meldplicht en voor de rechtsbescherming tegen sanctiebesluiten bij niet naleving van deze meldplicht aansluiting te zoeken bij het stelsel van de Wbp. Daarbij is onderkend dat er verschillen zijn tussen het stelsel van de Wbp en dat van de Telecommunicatiewet. Zo verschilt de regeling van de rechterlijke bevoegdheid en zijn er ook enkele kleine verschillen in de regels van procesrechtelijke aard, in het bijzonder voor wat betreft schorsende werking van het instellen van rechtsmiddelen. De Afdeling adviseert voor de procesrechtelijke voorschriften aansluiting te zoeken bij de Telecommunicatiewet en deze voorschriften ook op te nemen ten aanzien van de voorgestelde algemene meldplicht op grond van de Wbp. Dit advies is ten dele gevolgd. In navolging van het huidige artikel 15.12 van de Telecommunicatiewet wordt met de wijziging van artikel 71 van de Wbp (artikel I, onderdeel E) voorgesteld dat ook het instellen van beroep bij de rechter tegen een sanctiebesluit op grond van de voorgestelde meldplicht in de Wbp, schorsende werking heeft. Daarmee worden de procesrechtelijke regimes voor de beide meldplichten meer gelijk getrokken. Voor het toekennen van schorsende werking aan verzet tegen een dwangbevel (artikel 15.14 Tw) bestaat mijns inziens geen dwingende reden. Ingevolge artikel 4:116 Awb levert een dwangbevel een executoriale titel op, die met toepassing van de bepalingen van

het Wetboek van Burgerlijke Rechtsvordering kan worden tenuitvoergelegd. Ingevolge deze bepalingen schorst het aanhangig maken van een executiegeschil bij de rechtbank de executie niet. Wel kan de voorzieningenrechter op grond van artikel 438, tweede lid, Rv op verzoek de executie voor een bepaalde tijd of totdat op het geschil is beslist, schorsen. Bij het aanpassen van de wetgeving aan de algemene regeling over bestuursrechtelijke geldschulden in de Vierde tranche van de Awb is als uitgangspunt geformuleerd dat slechts indien specifieke omstandigheden daartoe noodzaken, in afwijking van Rv, bepaald kan worden dat het aanhangig maken van een executiegeschil van rechtswege de executie schorst. Zulke specifieke omstandigheden zijn hier, naar mijn mening, niet aan de orde.

4. Redactionele kanttekeningen

Aan de redactionele kanttekeningen van de Afdeling is gevolg gegeven.

Van de gelegenheid is gebruik gemaakt om enkele andere wijzigingen aan te brengen. Artikel III is in technische zin verbeterd; de keuze voor de rechtsgang van de Wbp voor bestuurlijke boetezaken met betrekking tot de meldplichten datalekken op grond van de Telecommunicatiewet was niet geheel correct vorm gegeven. Als gevolg van de inwerkingtreding van de Wet aanpassing bestuursprocesrecht per 1 januari 2013 is de daarop betrekking hebbende samenloopbepaling geschrapt.

Voorts is de memorie van toelichting op een aantal punten uitgebreid en geactualiseerd. Zo is met name paragraaf 2.4 aangepast aan enkele ontwikkelingen met betrekking tot aanpalende meldplichten op nationaal en Europees niveau. Voorts is in de artikelsgewijze toelichting waar relevant verwezen naar de op handen zijnde Commissieverordening betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (COCOM12-25REV2).

Ik moge U verzoeken, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken, het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Staatssecretaris van Veiligheid en Justitie

---

(1) Memorie van toelichting, paragraaf 2.4.
(2) Artikel 31, eerste lid, onder c, van de Wbp.
(3) Het voorgestelde artikel 22, vierde lid, onderdeel c, van de Wbp.
(4) Memorie van toelichting, paragraaf 2.1.
(5) Ter implementatie van artikel 7 van Richtlijn 95/46/EG.
(6) Memorie van toelichting, paragraaf 3.1, kopje "Onvoldoende mogelijkheden om bijzondere persoonsgegevens ten behoeve van derden te verwerken".
(7) Stcrt. 2009, nr. 51.
(8) Memorie van de toelichting, paragraaf 3.3, kopje "College van procureurs-generaal". Het betreft hier een reactie op het advies van het College van procureurs-generaal op het concept van dit voorstel. Het College betwijfelt ook het nut en de noodzaak van de voorgestelde regeling ten opzichte van de bestaande praktijk rondom het publiceren van dergelijke beelden door de politie. Zie het advies van 19 april 2012.

(9) Artikel 16 van de Wbp.
(10) Advies van 19 april 2012.
(11) Memorie van toelichting, paragraaf 3.3, kopje "College van procureurs-generaal".
(12) Memorie van toelichting, paragraaf 3.1, kopje "Onvoldoende mogelijkheden om bijzondere persoonsgegevens ten behoeve van derden te verwerken".
(13) Kamerstukken II 1997/98, 25 892, nr. 3, blz. 121.
(14) Memorie van toelichting, paragraaf 3.3, kopje "Nederlandse Orde van Advocaten".
(15) Memorie van toelichting, paragraaf 3.1, kopje "Mogelijkheden voor de plaatsing van beelden op internet door particulieren".
(16) Memorie van toelichting, paragraaf 3.3, kopje "Nederlandse Orde van Advocaten".
(17) In het voorgestelde artikel 22, zevende lid, van de Wbp wordt bepaald: "Bij algemene maatregel van bestuur worden regels gesteld met betrekking tot de verwerkingen, bedoeld in het vierde lid, onder a en c. Bij die maatregel kan worden bepaald dat de verwerking slechts plaatsvindt met instemming van een bij die maatregel aan te wijzen bestuursorgaaan [Sic] of andere autoriteit."
(18) COM(2012) 11 final, artikel 31.
(19) Het voorgestelde artikel 34a, eerste lid, van de Wpb.
(20) Memorie van toelichting, paragraaf 4.1.5.
(21) Memorie van toelichting, paragraaf 4.1.5.
(22) Daar is in de toelichting ook terecht op gewezen met betrekking tot de handhaving van artikel 13 van de Wbp, memorie van toelichting, paragraaf 4.1.13.
(23) Memorie van toelichting, paragraaf 4.1.5.
(24) Memorie van toelichting, paragraaf 5.2.
(25) Memorie van toelichting, paragraaf 4.1.5.
(26) Het voorgestelde artikel 66, tweede lid, van de Wbp.
(27) Het voorgestelde vierde lid van artikel 15.4 van de Telecommunicatiewet.
(28) Dit in afwijking van de algemene regel van artikel 438, tweede lid, van het Wetboek van Burgerlijke Rechtsvordering. De hoogte van de boete rechtvaardigt deze afwijking, zie Kamerstukken II 2006/07, 31 124, nr. 3, blz. 20 en 62 (Aanpassingswet Vierde tranche Awb).
(29) Memorie van toelichting, artikelsgewijs, Artikel II, onderdeel G.
(30) Zie artikel 71 van de Wbp.

Gehele tekst ontwerpregeling met toelichting (pdf, 173 kB)