1530

Openbaar Ministerie

College van Procureurs-Generaal

Voorzitter

Postbus 20305 2500 EH Den Haag

Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 (0)70 339 96 00
telefax +31 (0)70 339 98 51

0 BD

Staatssecretaris van Veiligheid en Justitie
mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Onderdeel	Beleid & Strategie
Contactpersoon	
Doorkiesnummer(s)	
E-mail	
Datum	19 april 2012
Ons kenmerk	PaG/B&S/16319
Uw kenmerk	5720007 11/6
Onderwerp	Advies concept wetsvoorstel Wet bescherming persoonsgegevens (camerabeelden en datalekken)

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen

Geachte heer Teeven,

Bij brief van 19 december 2012 heeft u het College van procureurs-generaal gevraagd te adviseren over een conceptwetsvoorstel wijziging Wet bescherming persoonsgegevens in verband met een ruimer gebruik van camerabeelden en het invoeren van een meldplicht voor datalekken voor alle diensten van de informatiemaatschappij.
In het eerste onderdeel van het wetsvoorstel wordt een rechtsgrondslag gecreëerd voor een kleine verruiming van het aantal gevallen waarin camerabeelden door particuliere beveiligingsorganisaties en individuele burgers mogen worden verwerkt.
In het tweede onderdeel van het wetsvoorstel wordt geregeld dat de verantwoordelijke voor de verwerking van de persoonsgegevens de verplichting krijgt het College bescherming persoonsgegevens onverwijld in kennis te stellen van een inbreuk op getroffen beveiligingsmaatregelen, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen zijn verbonden voor de persoonlijke levenssfeer van de betrokkene.
Het College heeft met belangstelling kennis genomen van het wetsvoorstel en is gaarne bereid daarover te adviseren.

Gebruik camerabeelden

In de memorie van toelichting wordt geschetst dat cameratoezicht het zichtbaar maken van criminaliteit en overlast bevordert, hetgeen bijdraagt aan een effectieve bestrijding daarvan. Camerabeelden van strafbare feiten blijken een nuttig hulpmiddel bij de opsporing van deze strafbare feiten. Het tonen van deze beelden aan het publiek kan een zinvolle ondersteuning betekenen van de opsporing. Het wetsvoorstel beoogt de privacywetgeving te wijzigen, zodat een wat ruimer gebruik van door particulieren vervaardigde camerabeelden mogelijk wordt gemaakt.

Het College kan zich voor een belangrijk deel vinden in hetgeen in de memorie van toelichting wordt gezegd over de toepassing van het cameratoezicht, ook als het gaat om door burgers vervaardigde camerabeelden. Het openbaar ministerie heeft forse ambities geformuleerd over het terugdringen van high impact crime zoals overvallen en ernstige vormen van overlast en criminaliteit in de wijk en de buurt. Een belangrijk element van deze aanpak is dat de overheid aan de burgers een duidelijk signaal afgeeft dat deze criminaliteit niet wordt getolereerd. De aanpak van deze criminaliteit is een gezamenlijke aanpak: nadrukkelijk worden burgers en bedrijven door het bestuur, politie en openbaar ministerie betrokken bij het oplossen van de problemen. Dat lukt alleen als burgers zien dat hun inspanning gepaard gaat met een zichtbare en effectieve reactie op criminaliteit van politie en openbaar ministerie. De inzet van het openbaar ministerie hangt samen met de keuzes die het bestuur maakt, gehoord de burgers en in overleg met partners. De inzet van cameratoezicht door particulieren en bedrijven kan een ondersteuning betekenen voor de opsporing van strafbare feiten. Daarvoor is nodig dat er goede afspraken worden gemaakt met op landelijk niveau bijvoorbeeld brancheverenigingen en op lokaal niveau met de plaatselijke winkeliersvereniging, bestuur van het winkelcentrum of het bestuur van een beveiligd appartementencomplex. Criminaliteit kan effectiever worden bestreden indien burgers en bedrijven het vervaardigde beeldmateriaal zo snel mogelijk ter beschikking kunnen stellen van de politie. Het College zal het voorstel voor een ruimer gebruik door particulieren van zelfvervaardigde camerabeelden tegen deze achtergrond bezien.

Kort samengevat wordt voorgesteld dat burgers zelfvervaardigde camerabeelden, waarop is te zien dat iemand een strafbaar feit pleegt, in beperkte kring in het openbaar mag publiceren en vertonen. Gedacht wordt aan publicatie op bijvoorbeeld beeldschermen en billboards in winkelcentra. Dit mag niet zomaar, de officier van justitie dient voor de publicatie toestemming te geven. Op deze wijze zou, volgens de memorie van toelichting, de omslachtige en langdurige procedure bij het College bescherming persoonsgegevens kunnen worden vermeden.

Het College meent dat het wetsvoorstel zoals het is ingericht op een aantal vragen en

bezwaren stuit. Als eerste kan de vraag worden gesteld of het voorstel in de praktijk enige meerwaarde heeft. In de Aanwijzing Opsporingsberichtgeving van het College van procureurs-generaal van 16 februari 2009 (Stcrt. 51), is een algemeen afwegingskader opgenomen voor het gebruik van diverse vormen van opsporingsberichtgeving. Aan de hand van proportionaliteit, subsidiariteit en de relatieve zwaarte van de inbreuk op de privacy worden beslissingen omtrent opsporingsberichtgeving genomen.
Uit de memorie van toelichting blijkt dat het toetsingskader dat in de Aanwijzing opsporingsberichtgeving is opgenomen ook behoort te gelden voor de in dit wetsvoorstel voorgestelde publicatie door een burger. Voorts wordt nadrukkelijk het standpunt ingenomen dat het primaat van de opsporing van strafbare feiten een overheidstaak blijft. Dit betekent dat in het geval een burger zelfvervaardigde camerabeelden aan het publiek wil tonen er hoe dan ook aangifte moet worden gedaan van een strafbaar feit en dat politie en justitie eerst de gelegenheid moeten krijgen de beelden te beoordelen op bruikbaarheid voor de opsporing.
Het College is het eens met deze uitgangspunten. Maar dan dringt de vraag zich op waarom het aan de burger moet worden overgelaten om bepaald beeldmateriaal te publiceren. Indien het openbaar ministerie aan de hand van de criteria van de Aanwijzing opsporingsberichtgeving oordeelt dat publicatie van dit beeldmateriaal in het belang van de opsporing is aangewezen, dan ligt het op de weg van politie en justitie om deze te publiceren in het kader van de opsporingsberichtgeving. Zij zijn daartoe in de meeste gevallen het best toe in staat omdat zij de berichtgeving van context kunnen voorzien of gebruik kunnen maken van speciale tools, zoals het gebruik van de app "De politie zoekt". Ook kan in gevallen die zich daarvoor lenen onder auspiciën van politie en justitie heel goed gebruik worden gemaakt van beeldschermen en billboards, door het beeldmateriaal te voorzien van een tekst zoals "de politie vraagt uw aandacht voor". Dat wordt ook nu al gedaan, in overleg met bijvoorbeeld stadiondirectie of een bestuur van een winkeliersvereniging.

Vervolgens is het onduidelijk wie eindverantwoordelijk is voor het publiceren van de camerabeelden en de wijze waarop dat is gedaan. Is dat de officier van justitie die toestemming heeft gegeven of de particulier die de beelden daadwerkelijk heeft gepubliceerd? In de memorie van toelichting wordt de indruk gewekt alsof publicatie van de camerabeelden door de burger geheel onder de verantwoordelijkheid van de officier van justitie is komen te vallen. Maar de verantwoordelijkheid voor het gebruik van camerabeelden is door de toestemming van de officier van justitie niet overgegaan van de burger naar het openbaar ministerie. Immers, de burger blijft de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens, daarin is geen verandering opgetreden. De verantwoordelijkheid voor de camerabeelden en wat hij daar mee doet blijft in alle gevallen liggen bij de burger die de camerabeelden in beheer heeft en zelf wil publiceren. Indien de burger de hem gegeven toestemming op

een onjuiste manier uitlegt, komen de gevolgen voor een eventuele onrechtmatige publicatie voor rekening van deze burger. Maar ook in het geval achteraf blijkt dat de toestemming van de officier van justitie onterecht is gegeven, bijvoorbeeld omdat ten tijde van de toestemming de beslissing op grond van onjuiste informatie is genomen, is de burger die publiceert eindverantwoordelijk. Dat maakt dat het voorstel leidt tot een ongewenst diffuus stelsel van verantwoordelijkheden.

Voorts merkt het College op dat het voorstel voor het openbaar ministerie een forse extra werklast betekent. Zeker in de grotere steden moet er rekening mee worden gehouden dat dagelijks met een aantal particulieren per geval moet worden besproken en beoordeeld of toestemming voor particuliere publicatie kan worden gegeven. De camerabeelden moeten worden bekeken en alvorens toestemming te verlenen moet worden afgestemd met de politie over de vraag of er aangifte is gedaan en zo ja of er mogelijk andere omstandigheden zijn die publicatie van de camerabeelden verhinderen. Ook zal dan van de officier van justitie worden verlangd dat hij bij het verlenen van toestemming rekening houdt met de belangen van derden die mogelijk ook op de camerabeelden zijn te zien.

In de memorie van toelichting wordt geen aandacht wordt geschonken aan het feit dat in het geval het met zekere regelmaat aan de burger zelf wordt overgelaten om camerabeelden te publiceren waarop een verdachte is te zien, deze burger (meestal het slachtoffer) in een kwetsbare positie kan worden gebracht. Het gebruik van camerabeelden door particulieren wordt aangeduid als "ondersteuning van de opsporing". Maar op het moment dat een burger zelf camerabeelden publiceert, met daarbij de vraag wie meer kan vertellen over de getoonde verdachte, is er geen sprake meer van ondersteuning van de opsporing, dan is er sprake van opsporing.
Het College wijst erop dat niet voor niets de opsporing van strafbare feiten exclusief in handen is gegeven van overheidsorganen. In de eerste plaats ter voorkoming van eigenrichting, maar ook ten behoeve van de bescherming van burgers. Met de opsporing en vervolging door politie en justitie wordt voorkomen dat burgers zelf met verdachten de confrontatie aan hoeven gaan. Deze bescherming kan in het gedrang komen indien burgers overgaan tot opsporing door middel van het beheren en publiceren van beeldmateriaal waarop een verdachte is te zien. Het is niet ondenkbaar dat na een aantal succesvolle publicaties verdachten zullen trachten om onder bedreiging van geweld publicatie van het beeldmateriaal te voorkomen of te verhinderen. De publicerende burger vormt dan immers een zelfstandige bedreiging voor de verdachte. Indien deze vrees wordt bewaarheid moet rekening worden gehouden met de mogelijkheid dat daarbij (nog meer) geweld tegen het slachtoffer wordt gebruikt.

Alles afwegende komt het College tot de conclusie dat aan dit onderdeel van het wetsvoorstel meer nadelen dan voordelen zijn verbonden. De onduidelijke verantwoordelijkheidsstructuur, de extra werklast voor het openbaar ministerie, de mogelijke nadelige effecten voor het slachtoffer zelf en de constatering dat een meerwaarde om de burger zelf het beeldmateriaal te laten publiceren zo goed als niet aanwezig is, maakt dat het College u adviseert om dit onderdeel van het wetsvoorstel te heroverwegen en niet in deze vorm verder in procedure te brengen.

Het College wil echter wel het streven ondersteunen om meer rendement te halen uit het door burgers en bedrijven toegepaste cameratoezicht, zodat kan worden bijgedragen aan een effectieve bestrijding van criminaliteit en overlast. De sleutel ligt naar het oordeel van het College echter bij de vraag of beeldmateriaal dat is verkregen door cameratoezicht zo snel mogelijk en zonder onnodige belemmeringen door de politie kan worden gebruikt in de opsporing. En precies op dit punt bestaat een knelpunt in de wetgeving.
Het is opsporingsambtenaren niet toegestaan om in alle gevallen zonder vordering van de officier van justitie ex artikel 126nd Sv beeldmateriaal van cameratoezicht te bekijken. Bijvoorbeeld in het geval van collega-winkeliers bij wie de overval of de winkeldiefstal niet is gepleegd maar waar de verdachten mogelijk ook zijn geregistreerd door aanwezige camera's. Opsporingsambtenaren zouden deze beelden graag ter plekke willen bekijken en eventueel meenemen indien blijkt dat voor de opsporing nuttige gegevens op het materiaal is vastgelegd. De Hoge Raad heeft echter uitgemaakt dat in al deze gevallen een vordering ex artikel 126nd Sv noodzakelijk is.[1] Dat heeft aanzienlijke administratieve lasten voor politie en openbaar ministerie tot gevolg en belemmert het snel kunnen werken.

Het College meent dat voor het verstrekken en gebruik van beeldmateriaal dat is gegenereerd door cameratoezicht van twee uitgangspunten moet worden uitgegaan. De burger zou niet na hoeven denken of hij ingevolge de Wet bescherming persoonsgegevens het beeldmateriaal al dan niet ten behoeve van de opsporing van strafbare feiten mag verstrekken aan de politie. Voor de politie zou er geen belemmering moeten zijn om snel over voor de opsporing relevant beeldmateriaal te kunnen beschikken. Beeldmateriaal dat in vrijwel alle gevallen graag ten behoeve van de opsporing wordt afgestaan. Dit kan worden bereikt door de opsporingsambtenaar in het Wetboek van Strafvordering de bevoegdheid toe te kennen de door cameratoezicht opgeslagen camerabeelden vormvrij bij de verantwoordelijke te vorderen. Deze lichte vorderingsbevoegdheid staat in een juiste verhouding tot de aard

[1] Zie HR 21-12-2010, LJN BL7688, waarin het ging om camerabeelden gemaakt in een supermarkt, waarop was te zien dat met een oude vrouw contact werd gemaakt door de mannen die haar later beroofden.

van deze opsporingsbevoegdheid. Er is immers geen sprake van een ernstige inbreuk op de persoonlijke levenssfeer van betrokkenen of derden. Introductie van deze vorderingsbevoegdheid heeft tot gevolg dat de burger in alle gevallen gerechtigd is de camerabeelden aan de politie ter beschikking te stellen. Hij dient immers aan een dergelijke vordering van de politie te voldoen. Op deze wijze is een wijziging van de Wet bescherming persoonsgegevens niet nodig.

Meldplicht datalekken

Met een zekere regelmaat komt het voor dat persoonsgegevens openbaar worden omdat de verantwoordelijke onvoldoende beveiligingsmaatregelen heeft genomen om de persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, of door een inbreuk op deze beveiligingsmaatregelen. Om die reden worden alle diensten van de informatiemaatschappij onderworpen aan een meldplicht voor inbreuken op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens. Vanwege het ontbreken van een directe relatie met de strafrechtelijke handhaving ziet het College voor dit onderdeel van het wetsvoorstel geen aanleiding tot het maken van enige op- of aanmerking.

Hoogachtend

Het College van procureurs-generaal

H.J. Bolhaar

WRR 145340

0 BD

de Rechtspraak

Raad voor de rechtspraak

Aan de minister van Veiligheid en Justitie
Mr. I. W. Opstelten
Postbus 20301
2500 EH DEN HAAG

Directie Strategie en Ontwikkeling

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

t (070) 361 97 23
f (070) 361 97 46
www.rechtspraak.nl

datum 7 juni 2012
contactpersoon
doorkiesnummer
faxnummer
e-mail
ons kenmerk UIT 5380 S&O / KA
uw kenmerk -
onderwerp Adviesaanvraag Wetsvoorstel gebruik camerabeelden en meldplicht datalekken

Geachte heer Opstelten,

Bij brief van 19 december 2011 welke ik heb ontvangen op 22 december 2011 verzocht u de Raad voor de rechtspraak (de "**Raad**") advies uit te brengen inzake het Wetsvoorstel "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)". Hierna te noemen het **"wetsvoorstel"**. Dit wetsvoorstel heeft u geplaatst ter internetconsultatie.

Als eerste mijn excuses dat deze formele reactie richting u wegens onvoorziene omstandigheden vertraging heeft opgelopen.

In dit wetsvoorstel wordt een 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.

Gehoord de gerechten, adviseert de Raad als volgt.[1]

[1] De Raad voor de rechtspraak heeft op grond van artikel 95 Wet op de rechterlijke organisatie een wettelijke adviestaak met betrekking tot nieuwe wets- en beleidsvoorstellen die gevolgen hebben voor de rechtspraak. De adviezen worden vastgesteld na overleg met de gerechten. De Raad voor de rechtspraak is een adviescollege in de zin van artikel 79 en 80 van de Grondwet. Bij het opstellen van zijn adviezen beoordeelt de Raad de voorgenomen wet- en regelgeving in het bijzonder op de gevolgen voor de organisatie en de werklast van de gerechten en op de (praktische) toepasbaarheid en uitvoerbaarheid. Rechters zijn bij de behandeling van individuele zaken niet gebonden aan de inhoud van de wetgevingsadviezen van de Raad voor de rechtspraak.

de Rechtspraak

Raad voor de
rechtspraak

datum 7 juni 2012
kenmerk UIT 5380 S&O / KA
pagina 2 van 2

Advies
Het wetsvoorstel voorziet in bepalingen die de rechtsbescherming van de betrokkene nader invullen. Daarnaast voorziet de Raad geen substantiële gevolgen voor de werklast.

Daarmee geeft het wetsvoorstel geen aanleiding tot het maken van op- en aanmerkingen. Indien in een later stadium nog wijzigingen in het wetsvoorstel worden aangebracht die gevolgen hebben voor de rechtspleging dan wordt de Raad graag in de gelegenheid gesteld aanvullend te adviseren.

Hoogachtend,

Mr. J.C. van Dijk
Lid van de Raad voor de rechtspraak

ICT~OFFICE

Staatssecretaris van Veiligheid & Justitie
De heer mr. F. Teeven, MPM
Postbus 20301
2500 EH DEN HAAG

Woerden, 29 februari 2012

Betreft : reactie ICT~Office op wetsvoorstel wijziging WBP, meldplicht voor datalekken
Kenmerk : 20120229/BT/BP

Geachte heer Teeven,

In uw brief van 19 december 2011 heeft u ICT~Office gevraagd te reageren op de consultatie van het wetsvoorstel Wet Bescherming Persoonsgegevens (Wbp). Graag maakt ICT~Office, de brancheorganisatie voor ICT- en Telecombedrijven in Nederland, gebruik van deze mogelijkheid. ICT~Office beperkt haar reactie tot het voorstel omtrent de meldplicht voor datalekken.

Recent heeft de Europese Commissie voorstellen gedaan voor een Verordening inzake de gegevensbescherming. In dit voorstel wordt een meldplicht voor datalekken voorzien. Europese harmonisatie is zeer gewenst in dit kader, aangezien niet alleen het internet geen grenzen kent, maar ook veel bedrijven buiten de landsgrenzen actief zijn. ICT~Office verzoekt u om in Nederland geen nieuwe privacyregelgeving te introduceren die binnen afzienbare tijd zal worden vervangen door Europese regelgeving. Dit verdubbelt de implementatielasten van het bedrijfsleven en creëert veel onduidelijkheid.

ICT~Office vraagt u om het Nederlands wetsvoorstel te gebruiken als inzet in het wetgevingsproces in Brussel opdat de Verordening aansluit bij de Nederlandse behoefte. In reactie op het huidige wetsvoorstel wil ICT~Office u vragen om deze meer in lijn te brengen met het beoogde doel: het voorkomen van datalekken en het minimaliseren van de impact op de betrokkene indien er onverhoopt toch een datalek is.

In de bijlage gaat ICT~Office uitgebreid in op het huidige voorstel met opmerkingen of suggesties. Deze opmerkingen kunnen als volgt worden samengevat:

- ICT~Office ziet een meldplicht als signalerende maatregel voor wanneer het onverhoopt fout gaat in de beveiliging van gegevens, die verantwoordelijken bewuster maakt van het belang van transparantie bij een datalek. De meldplicht zal echter leiden tot een forse verzwaring van de lasten van het bedrijfsleven en van de toezichthouder Cbp zonder dat deze meldplicht de beveiliging van gegevens direct verhoogt.
- De verhouding met andere, bestaande en nog uit te werken, meldplichten is ICT~Office nog onduidelijk. Vooral de relatie met de nog uit te werken meldplicht *security breaches* roept vragen op.

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@ictoffice.nl
www.ictoffice.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

ICT~OFFICE

- Beveiligd zijn is niet hetzelfde als 100 procent veilig zijn. Een verantwoordelijke kan passende maatregelen hebben genomen om persoonsgegevens te beveiligen - en daarmee de Wbp naleven - en toch geconfronteerd worden met een datalek. De samenleving zal de beveiliging echter als te laag ervaren. Dat vergroot de impact van een meldplicht. ICT~Office vraagt het kabinet om in de opzet van en toelichting op de meldplicht sterkere aandacht te geven hieraan.

- Een melding moet worden gedaan als er - kort gezegd - een inbreuk is geconstateerd op de beveiligingsmaatregelen. Organisaties die hun beveiliging niet goed op orde hebben zullen deze inbreuken niet snel opmerken, terwijl het risico bij deze organisaties het grootst is. De meldplicht geeft geen positieve prikkels aan organisaties om die situatie te veranderen. Om deze paradox tegen te gaan, stelt ICT~Office voor om prikkels in te bouwen, bijvoorbeeld door bij aantoonbaar adequate beveiliging een alternatief toezichts- en/of meldingsregime mogelijk te maken.

- In algemene zin pleit ICT~Office voor proportionaliteit bij een verplichting tot melding en vraagt alleen die (zware) gevallen onder de meldplicht te laten vallen waaraan het Cbp ook daadwerkelijk navolging kan geven.

- ICT~Office pleit daarbij voor een heldere afbakening van de reikwijdte van de meldplicht en het opstellen van duidelijke criteria waaraan wordt getoetst, zowel wanneer het een inbreuk betreft als wanneer er sprake is van aanmerkelijk risico en nadelige gevolgen voor de betrokkene.

- De meldplicht vraagt om onverwijlde melding aan toezichthouder en betrokkene. ICT~Office stelt voor om bij een onverwijlde melding aan de toezichthouder een verantwoordelijke de ruimte te laten om eerst de aard en omvang van de inbreuk te onderzoeken. ICT~Office stelt daarnaast voor om de melding aan betrokkene te veranderen in 'zo spoedig als redelijkerwijs mogelijk'. Hierdoor blijft er ruimte om per incident de beste aanpak te bepalen.

- ICT~Office is tevreden met de insteek om meldingen aan de toezichthouder niet te publiceren. Wel ziet ICT~Office te weinig waarborgen om meldingen echt vertrouwelijk te houden. ICT~Office pleit ervoor dat de gehele melding als bedrijfsvertrouwelijk wordt aangemerkt in het kader van de Wet Openbaarheid Bestuur.

- Tot slot vraagt ICT~Office om een hernieuwd onderzoek naar de administratieve lasten, bij voorkeur uitgevoerd door Actal. ICT~Office vindt de huidige inschatting weinig realistisch.

ICT~Office is graag bereid om de opmerkingen en suggesties op het huidige wetsvoorstel nader toe te lichten.

Met vriendelijke groet,
ICT~Office

mr. Sylvia J.M. Roelofs
algemeen directeur

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@ictoffice.nl
www.ictoffice.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

ICT~OFFICE

Bijlage: Reactie ICT~Office op wetsvoorstel meldplicht voor datalekken

De reactie van ICT~Office op het wetsvoorstel meldplicht voor datalekken (hierna: de meldplicht) is uitgesplitst in twee onderdelen: algemene opmerkingen over het voorstel voor de meldplicht en enkele specifieke opmerkingen gerelateerd aan artikelen van het wetsvoorstel.

Meldplicht kan leiden tot betere bewustwording

ICT~Office onderschrijft het belang dat verantwoordelijken transparant zijn over de wijze waarop zij met gegevens van klanten omgaan, ook als het onverhoopt een keer mis gaat. Verantwoordelijken die hierover een goede relatie opbouwen met hun klanten kunnen in beginsel rekenen op meer begrip dan verantwoordelijken die dat niet doen. Als een meldplicht op een goede manier wordt opgezet en uitgevoerd kan een meldplicht helpen om verantwoordelijken bewuster te laten zijn van het feit dat transparantie helpt om het vertrouwen te versterken. Tevens zou het ook een bijdrage kunnen leveren aan de maatschappelijke bewustwording van het feit dat aan de verwerking van gegevens ook risico's zijn verbonden die nooit voor 100 procent zijn af te dekken.

Vooral een signalerende maatregel

ICT~Office ziet in een meldplicht kansen voor een betere beveiliging (voorkomen van datalekken) en het minimaliseren van de impact op de betrokkene als er toch onverhoopt een datalek is. ICT~Office staat echter nog niet onverdeeld achter het huidige wetsvoorstel. Een meldplicht zal leiden tot een forse verzwaring van de lasten van het bedrijfsleven en het Cbp zonder dat dit de effectiviteit van de gegevensbescherming vergroot. ICT~Office vindt een meldplicht voornamelijk een signalerende maatregel die erop is gericht om te repareren wanneer het onverhoopt fout gaat, terwijl de aandacht vooral uit zou moeten gaan naar een sterkere preventie op het terrein van de beveiliging.

Verhouding met andere meldplichten: Europese Verordening leidend

ICT~Office ziet een wildgroei aan meldplichten ontstaan. Naast de reeds bestaande beperkte meldplicht voor bijzondere situaties, volgt op afzienbare termijn een meldplicht voor de aanbieders van elektronische communicatiediensten, volgt dit wetsvoorstel voor een algemene meldplicht en volgt er nog een uitwerking van de door de Tweede Kamer gevraagde meldplicht bij *security breaches* (inbreuken op de beveiligingsmaatregelen). Tevens is door de Europese Commissie in januari 2012 een Verordening inzake de gegevensbescherming gepubliceerd die ook een meldplicht datalekken introduceert. Deze Europese meldplicht zal snel na invoering van een Nederlandse meldplicht van kracht worden en daarmee de Nederlandse werkelijkheid inhalen.

ICT~Office vraagt zich daarom sterk af waarom een eigen Nederlandse algemene meldplicht datalekken op dit moment nodig is. ICT~Office stelt voor het huidige wetsvoorstel te gebruiken om de Europese meldplicht in lijn te krijgen met het voorziene Nederlandse voorstel en stelt tevens voor om de Nederlandse meldplicht samen te laten vallen met de invoering van de Europese privacyregels.

Beveiligd zijn is niet hetzelfde als 100 procent veilig zijn

Een verantwoordelijke kan de volgens de Wbp geëiste passende maatregelen hebben genomen om persoonsgegevens te beschermen – en daarmee de wet volledig naleven – en toch geconfronteerd worden met een datalek. Bij het ontdekken van een datalek zal het algemene oordeel van betrokkenen en in de samenleving echter zijn dat de gegevensbeveiliging te laag was. Beveiligen is echter niet absoluut maar het zoeken naar een balans op basis van een risicoafweging. Het wetsvoorstel lijkt weinig rekening te houden dat met de invoering van de meldplicht deze te ongenuanceerde perceptie over beveiliging onbedoelde neveneffecten kan hebben voor het vertrouwen in de digitale samenleving. Dit wordt mogelijk nog verstrekt als te vaak melden tot een 'meldingsvermoeidheid' gaat leiden waardoor minder adequaat wordt geregeerd op echte problemen.

Tevens ziet ICT~Office het als risico dat bij gevallen die buiten de scope vallen van wat de wetgever beoogt met dit wetsvoorstel, toch door de samenleving wordt verwacht dat dit door de verantwoordelijke wordt gemeld. Een meldplicht kan wel wettechnisch afgebakend worden maar zal in de praktijk weinig afbakening kennen. Dat creëert een nog grotere impact van het concept meldplicht.

ICT~Office constateert daarnaast een in onze ogen zorgelijke tendens waarbij verantwoordelijken die openheid betrachten direct worden geconfronteerd met extra (negatieve) aandacht, nog voordat de verantwoordelijke zelf zijn incidentrespons heeft kunnen afronden. De samenleving moet duidelijk nog wennen aan het idee dat gegevens soms helaas toegankelijk blijken voor onbevoegden. Gecombineerd met de bovenstaande constateringen leidt dit ertoe dat een verantwoordelijke nooit juist zal kunnen handelen.

› ICT~Office verzoekt het kabinet om in de opzet van en toelichting op de wet een sterkere aandacht te geven hieraan, zodat de juiste verwachting ontstaat van een meldplicht en de context waarvoor deze is bedoeld. Daarnaast vraagt ICT~Office het kabinet om een sterkere afkeuring richting diegenen die inbreken in andermans systemen en gegevensbestanden.

Positieve prikkels nodig voor beveiligingsmaatregelen

Een meldplicht kan bijdragen aan een sterkere beveiliging van systemen en gegevens als deze de juiste prikkels geeft voor het steeds beter beveiligen. Het huidige wetsvoorstel regelt dat bij een inbreuk op de beveiligingsmaatregelen er een melding moet plaatsvinden. Dat veronderstelt dat een verantwoordelijke eerst moet constateren dat een inbreuk heeft plaatsgevonden. Een verantwoordelijke die zich goed beveiligt en veel kennis over beveiliging in huis heeft, zal eerder opmerken dat er zich een inbreuk heeft voorgedaan dan een verantwoordelijke die onvoldoende aandacht besteedt aan het beveiligingsvraagstuk.

De paradox van de meldplicht is dat het risico op verlies van persoonsgegevens juist het grootst is bij verantwoordelijken die onvoldoende hebben geïnvesteerd in beveiliging en daardoor inbreuken op de beveiliging ook minder snel zullen opmerken. Wanneer een inbreuk niet wordt opgemerkt, kan deze echter ook niet worden gemeld. Buiten het voorkomen van (abstracte) reputatieschade geeft het huidige wetsvoorstel geen prikkels om deze situatie te veranderen. Het beter zicht hebben op eigen systemen (en daarmee monitoren van inbreuken) moet lonen voor een verantwoordelijke.

Juist verantwoordelijken die veel zicht hebben op eigen systemen, zullen inbreuken sneller opmerken en daarmee beter kunnen melden bij het Cbp. Wanneer deze meldingen echter publiek zouden worden, kan dat een verkeerd beeld geven van het daadwerkelijke beveiligingsniveau van verantwoordelijken. Met andere woorden: de verantwoordelijke doet beter zijn best met als mogelijk gevolg dat daardoor een slechtere indruk ontstaat. In lijn met de hierboven geschetste paradox stelt ICT~Office voor dat verantwoordelijken die hun bevelliging aantoonbaar adequaat hebben georganiseerd op een andere wijze worden benaderd en beoordeeld door het Cbp dan verantwoordelijken die dat niet adequaat hebben georganiseerd. ICT~Office stelt voor om te onderzoeken of verantwoordelijken die hun beveiliging volgens de eisen van de Wbp hebben ingericht in een alternatief toezichts- en/of meldingsregime terecht kunnen komen. Dit zou bijvoorbeeld kunnen door een functionaris gegevensbescherming een plek te geven in dat lichtere regime, of door alleen een register van incidenten bij te hoeven houden.

› ICT~Office stelt voor de inrichting van de meldplicht datalekken de verantwoordelijke aanmoedigt met positieve prikkels om beveiligingsmaatregelen te treffen, bijvoorbeeld door een alternatief toezichts- en/of meldingsregime mogelijk te maken.

Scope van de meldplicht

ICT~Office steunt de intentie om alleen de zwaardere gevallen onder een meldplicht te laten vallen, maar vindt de afbakening met de niet-zware gevallen nog te abstract. Daardoor is het aan verantwoordelijken zelf ter beoordeling wanneer men denkt binnen de afbakening te vallen. Dat leidt tot onzekerheid. ICT~Office pleit voor concrete criteria die duidelijk stellen in welke gevallen een verantwoordelijke onderhevig is aan de meldplicht en in welke gevallen niet. Dit is in het kader van de handhaving ook noodzakelijk voor de vraag wanneer een boete wordt opgelegd bij het niet-nakomen van de meldplicht.

In het voorstel is ervoor gekozen om een meldplicht te laten gelden wanneer er een inbreuk is op de maatregelen, bedoeld in artikel 13 Wbp, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer zijn verbonden. ICT~Office heeft vragen bij verschillende onderdelen van deze bepaling.

Inbreuk op de maatregelen, bedoeld in artikel 13 Wbp

Het gaat hierbij om een inbreuk op "passende technische en organisatorische maatregelen" bedoeld om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Dat is een dusdanige brede omschrijving dat onduidelijk is welke digitale of fysieke inbreuken hieronder vallen. Moeten bijvoorbeeld een brand in een serverruimte, of een schoonmaker die niet geautoriseerd was voor toegang tot bepaalde ruimtes, als 'inbreuken op de maatregelen' worden beschouwd? Ook in dit geval leiden meer beveiligingsmaatregelen er overigens toe dat er eerder sprake zal zijn van een inbreuk op die maatregelen. Een brede interpretatie van deze bepaling brengt grote lasten mee. Weliswaar kan uit onderzoek van de verantwoordelijke blijken dat geen risico bestaat voor de persoonsgegevens, maar door het op te nemen binnen de definitie leidt het er wel toe dat ieder van dit soort incidenten onderzocht moet worden door de verantwoordelijke.

Aanmerkelijk risico op verlies of onrechtmatige verwerking en nadelige gevolgen
Het is ICT~Office niet duidelijk wanneer de afweging moet worden gemaakt dat er sprake is van een aanmerkelijk risico op verlies. De wijze waarop dit is verwoord leidt ertoe dat het niet gaat om een daadwerkelijk risico of een daadwerkelijk verlies aan data maar al dat een inbreuk leidt tot een vergroting van het risico. De meeste inbreuken zullen tot een vergroting van het risico leiden. Ook de term 'onrechtmatige verwerking' zou verder uitgewerkt kunnen worden. Met de abstracte kaders van de Wbp kan al snel sprake zijn van een onrechtmatige verwerking.

De passage 'nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer' is een dusdanige open norm dat deze moeilijk in te vullen zal zijn. ICT~Office is overigens benieuwd wat moet worden verstaan onder nadelige gevolgen voor de persoonsgegevens. ICT~Office stelt voor de nadelige gevolgen te beperken tot alleen de persoonlijke levenssfeer.

› ICT~Office pleit voor een heldere afbakening van de reikwijdte van wanneer een melding moet worden gedaan en het opstellen van duidelijke criteria waaraan wordt getoetst, zowel wanneer het een inbreuk betreft als wanneer er sprake is van aanmerkelijk risico en van nadelige gevolgen.

'Onverwijld' melden van een datalek aan het Cbp
De meldplicht datalekken stelt dat bij een inbreuk op de maatregelen het Cbp onverwijld in kennis wordt gesteld en dat de betrokkene ook onverwijld in kennis moet worden gesteld. ICT~Office vraagt zich af hoe deze tijdsindicatie moet worden geïnterpreteerd. Er zit een afruil tussen de tijdigheid van informatievoorziening en de zorgvuldigheid daarvan. Bij constatering van de inbreuk zal namelijk eerst goed moeten worden onderzocht wat de inbreuk precies was en vervolgens moet worden afgewogen of sprake is van een 'aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens' en vervolgens of aan deze onrechtmatige verwerking ook 'nadelige gevolgen zijn verbonden aan de persoonlijke levenssfeer van de betrokkene'.

Bij een melding aan het Cbp moet voorkomen worden dat ook ieder vermoeden van een datalek moet worden gemeld. Dat levert niet alleen verhoogde administratieve lasten op maar zonder goede duiding en informatie van een incident kan dat ook leiden tot een onjuiste inschatting bij het Cbp en daarmee leiden tot een onnodige of onjuiste aanwijzing.

› ICT~Office stelt voor om onverwijld dusdanig in te interpreteren in de memorie van toelichting dat deze ruimte laat om eerst te beoordelen wat de inbreuk is, en daarna te melden.

'Zo spoedig als redelijkerwijs mogelijk' melden van een datalek aan de betrokkene
Een onverwijlde melding aan de betrokkene wil ICT~Office graag veranderd zien in "zo spoedig als redelijkerwijs mogelijk". Naast de bovengenoemde redenen van een zorgvuldig onderzoek naar de impact van een datalek op de persoonlijke levenssfeer van de betrokkene, geldt ook dat bij kwaadwillende bedoelingen van criminelen het in het belang van de bestrijding van die criminelen kan zijn om betrokkenen pas later te informeren. Ieder incident moet op een eigen manier worden opgelost. Verantwoordelijken hebben de ruimte nodig om (verergering van de) gevolgen van een

datalek te voorkomen. De wet zal hen die ruimte moeten geven. Of de verantwoordelijke de ruimte goed heeft gebruikt, is achteraf ter beoordeling van het Cbp. Deze aanpassing geeft het Cbp in tijd ook de gelegenheid om te beoordelen of er sprake is van gepaste technische beschermings-maatregelen die persoonsgegevens onbegrijpelijk heeft gemaakt. Pas na deze beoordeling van het Cbp kan de betrokkene worden geïnformeerd (artikel 34a lid 6 versus artikel 34a lid 2).

Hetgeen bepaald in artikel 34a lid 2 veronderstelt overigens dat de verantwoordelijke precies weet welke personen in zijn gegevensverwerking zijn opgenomen en dat de desbetreffende database reconstrueerbaar is. Dat is niet altijd het geval, met name niet wanneer de inbreuk gepaard gaat met gegevensverminking. ICT~Office stelt voor om artikel 34a lid 2 in die zin te nuanceren.

› ICT~Office stelt voor om flexibiliteit te houden in het wetsvoorstel over het moment van melden en 'onverwijld' in artikel 34a lid 2 aan te passen naar 'zo spoedig als redelijkerwijs mogelijk'.

Relatie tussen verantwoordelijke en bewerker

ICT~Office onderschrijft het in het voorstel opgenomen uitgangspunt om ook in het geval van uitbesteding de meldplicht bij de verantwoordelijke te laten rusten. Dat sluit aan bij de praktijk waarbij vaak nu al tussen verantwoordelijke en bewerker contractueel is geregeld dat incidenten door de bewerker aan de verantwoordelijke worden gemeld. Dit hoeft in de ogen van ICT~Office niet extra te worden geregeld in een aanpassing van artikel 14.

ICT~Office heeft enige zorg dat de bewerker via zijn relatie met de verantwoordelijke wel de verantwoordelijkheid (en eventuele financiële aansprakelijkheid) van de gevolgen van datalekken wordt toegeschoven, vooral in die gevallen waar een verantwoordelijke heeft verzuimd om contractueel voldoende maatregelen aan de bewerker toe te wijzen voor de bescherming van persoonsgegevens.

Respons van het Cbp

Er worden op jaarbasis ongeveer 66.000 meldingen verwacht in het kader van de meldplicht. In de memorie van toelichting staat dat het Cbp slechts een beperkt deel daarvan kan onderzoeken. Gegeven het doel van de meldplicht moet worden afgevraagd waarom het Cbp niet alle zaken die binnenkomen in onderzoek neemt. Dat betekent dat voor al die gevallen die het Cbp niet onderzoekt, de melding slechts een papieren exercitie en administratieve handeling is geweest. Daar heeft het Cbp, noch de betrokkene, noch de verantwoordelijke baat bij. In de Memorie van Toelichting moet duidelijk worden welke navolging wordt gegeven aan die meldingen waar het Cbp geen concrete actie op kan ondernemen.

› ICT~Office pleit ervoor om de criteria voor het doen van een melding dusdanig worden aangepast dat het Cbp alleen die meldingen ontvangt waaraan zij ook navolging kan geven.

Aanwijzingen door het Cbp en aansprakelijkheid

In de aanhef van de Memorie van Toelichting wordt aangegeven dat het Cbp door de verantwoordelijke moet worden geïnformeerd opdat het Cbp kan beoordelen of een onderzoek of het

geven van aanwijzingen noodzakelijk is. Het is ICT~Office niet duidelijk op basis waarvan dit onderzoek zou moeten plaatsvinden en wat de aard is van de aanwijzingen of het interveniëren is. ICT~Office vindt het ongewenst als het Cbp aan een melder concrete aanwijzingen kan geven hoe te reageren op een incident. Het Cbp moet vooral ondersteuning bieden en (vrijblijvend) adviseren. Het is aan de verantwoordelijke zelf om te bepalen welke acties nodig zijn in reactie op een inbreuk op de maatregelen.

Als het Cbp toch directe aanwijzingen kan geven over de acties die nodig zijn, dan vraagt ICT~Office zich af of het Cbp aansprakelijk kan worden gesteld voor schade die ontstaat door een aanwijzing van het Cbp die tot grotere schade heeft geleid dan wanneer de verantwoordelijke eigen keuzes had kunnen maken of waardoor acties uitblijven die de schade vergroten.

Geen naming & shaming, wel goede algemene adviezen

ICT~Office leidt uit het wetsvoorstel af dat meldingen niet openbaar zullen worden gemaakt door het Cbp. ICT~Office steunt dit standpunt. Naming & shaming door het Cbp is uiterst onwenselijk, en zelfs contraproductief. Om het leren van andere incidenten te bevorderen, zou het Cbp in samenwerking met het Nationaal Cyber Security Centrum periodiek adviezen kunnen publiceren over het beschermen tegen veel voorkomende incidenten. Dit kan het Cbp doen op basis van alle meldingen die zij ontvangt.

› ICT~Office stelt voor dat het Cbp voor adviezen over het voorkomen van incidenten samenwerkt met het Nationaal Cyber Security Centrum.

Sanctionering

ICT~Office ziet weinig in het idee van een bestuurlijke boete wanneer niet aan de meldplicht wordt voldaan. Een boete is niet de manier om verantwoordelijken te dwingen om te melden. Het zorgt alleen voor een vergroting van de discussie of een melding wel of niet binnen de afbakening valt en voor de discussie of een verantwoordelijke een inbreuk heeft opgemerkt. Energie wordt daarmee gestoken in het instrument van de meldplicht en niet in de verhoging van beveiligingsmaatregelen. In lijn met eerdere opmerkingen zullen veel verantwoordelijken pas in een later stadium, of helemaal niet, opmerken dat een inbreuk heeft plaatsgevonden. ICT~Office vraagt zich af hoe het Cbp bij het uitblijven van een melding zal handhaven, bijvoorbeeld wanneer een datalek niet is opgemerkt.

Sanctionering leidt er bovendien toe dat verkeerde overwegingen een rol kunnen gaan spelen bij het al dan niet melden van een datalek. Juist voor die verantwoordelijken die hun beveiliging wel op orde hebben, leidt sanctionering tot een afweging om sneller te melden om zeker te zijn dat hen achteraf geen boete wordt toebedeeld. Dit vergroot de lastendruk bij bedrijven maar ook bij het Cbp.

Vertrouwelijkheid

Het wetsvoorstel maakt niet duidelijk welke waarborg de verantwoordelijke heeft dat de door de verantwoordelijke aan het Cbp verstrekte gegevens vertrouwelijk worden behandeld. In het kader van laagdrempeligheid van melden zal vertrouwelijkheid gegarandeerd moeten worden. Voorkomen moet worden dat verantwoordelijken die in vertrouwen een melding doen bij het Cbp via een omweg alsnog in de media komen met hun melding, zeker voor die gevallen waarin er geen noodzaak is tot melden aan de betrokkenen.

Om het doel van de meldplicht te bereiken moet vertrouwelijkheid worden gegarandeerd. Het moet niet mogelijk zijn om via een WOB-verzoek meldingen van bedrijven en overheidsinstanties te achterhalen. Dit geeft een zeer negatieve prikkel aan het doen van meldingen. ICT~Office verzoekt met nadruk dat de melding als geheel als bedrijfsvertrouwelijk in de zin van artikel 10, eerste lid, onder c, van de Wet openbaarheid bestuur kan worden aangemerkt en niet alleen dat dit kan met gegevens binnen een melding.

In de memorie van toelichting wordt in paragraaf 4.4 de verhouding met het strafrecht besproken. Daarin wordt niet duidelijk dat de verantwoordelijke zelf de aangifte moet doen en niet dat het Cbp verstrekte gegevens zonder afstemming met de verantwoordelijke aan het Openbaar Ministerie doorgeeft. Welke waarborgen geeft het kabinet dat het Cbp de verkregen gegevens niet ongevraagd doorgeeft naar het Openbaar Ministerie?

› ICT~Office pleit ervoor dat de gehele melding als bedrijfsvertrouwelijk in het kader van de Wet Openbaarheid Bestuur kan worden aangemerkt, of dat andere voorzorgsmaatregelen worden getroffen die de vertrouwelijkheid van meldingen garanderen.

Internationale vraagstukken

De meldplicht op het gebied van de Wbp sluit niet uit dat ingeval van een datalek de verantwoordelijke op grond van buitenlandse wetgeving ook een meldplicht heeft jegens buitenlandse instanties en/of in het buitenland woonachtige betrokkenen. Een cumulatie van meldplichten kan aanzienlijke lasten met zich meebrengen, zeker wanneer die niet op elkaar zijn afgestemd. Om die reden verzoekt ICT~Office de wetgever om zich te buigen over de problematiek van de samenloop van Nederlandse en buitenlandse meldplichten. In de memorie van toelichting wordt geen inzicht gegeven hoe de Nederlandse wetgever hiermee om wenst te gaan. ICT~Office zou graag verhelderd zien hoe gehandeld moet worden in geval van een datalek met een grensoverschrijdend karakter.

Aansprakelijkheid / financiële effecten

In de memorie van toelichting wordt toegelicht dat het doen van een kennisgeving aan de betrokkene de verantwoordelijke op zichzelf genomen niet ontheft van eventuele burgerrechtelijke aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar niet of niet voldoende naleven van de verplichting neergelegd in artikel 13 van de Wbp. In de praktijk zal echter blijken dat betrokkenen schade die zij (denken te) hebben geleden als gevolg van het datalek alsnog zullen proberen te verhalen op de verantwoordelijke, ook al zijn de verplichtingen neergelegd in artikel 13 van de Wbp nageleefd. Dat leidt tot een verzwaring van de last bij verantwoordelijken.

ICT~Office pleit ervoor dat in de memorie van toelichting steviger wordt uitgesproken dat wanneer een verantwoordelijke de verplichtingen in artikel 13 naleeft het voor betrokkenen niet mogelijk is om op basis van de Wbp schade te verhalen van een eventueel datalek. Dit ter voorkoming van een claimcultuur. Daarnaast bepleit ICT~Office een niet-aansprakelijkheid voor schade die ontstaat als een betrokkene de in een melding aan hem aangeraden maatregelen niet opvolgt. Dit stimuleert verantwoordelijken om te zorgen dat de juiste maatregelen worden getroffen voor beveiliging van gegevens en stimuleert een snellere melding aan betrokkenen (positieve prikkels).

Nalevingskosten en administratieve lasten
ICT~Office vindt de berekening van de administratieve lasten weinig realistisch. Het al dan niet hebben van een meldplicht bepaalt niet de mate waarin verantwoordelijken transparant zouden moeten zijn naar hun klanten. Maar wel zorgt een meldplicht dat verantwoordelijken extra lasten ervaren doordat:

- Verantwoordelijke en bewerker extra onderzoeksinspanning moeten plegen om te bepalen of er een meldingsplicht geldt,
- Alle potentiële (grote, maar ook zeer kleine) inbreuken in beginsel beoordeeld moeten worden om te zien of melding noodzakelijk is (die lasten verzwaren nu de reikwijdte nog onduidelijk is)
- Zowel verantwoordelijke als bewerker een organisatorische systematiek moeten inrichten gericht op melden.
- de aanwijzingen van het Cbp kunnen leiden tot extra kosten zonder dat dit leidt tot een betere bescherming van gegevens of betere opvolging van een incident
- in navolging van het hierboven vermelde verantwoordelijken extra kosten gaan maken doordat een meldplicht impliceert dat schade verhaald kan worden op de verantwoordelijke.

De toets op de administratieve lasten is gebaseerd op een onderzoek gedaan ter voorbereiding van het wetsvoorstel tot wijziging van de Telecommunicatiewet. ICT~Office heeft in de consultatie toentertijd reeds gewezen op de onrealistische berekening van de administratieve lasten van de meldplicht.

› ICT~Office vraagt om een hernieuwd onderzoek naar de administratieve lasten, bij voorkeur uitgevoerd door Actal.

Specifieke artikelgerichte opmerkingen

Hierin worden niet de opmerkingen meegenomen die reeds hierboven zijn vermeld.

Artikel I

Artikel 34a lid 5
Het is niet duidelijk wat een 'behoorlijke en zorgvuldige informatievoorziening' is. ICT~Office vindt dat de kosten voor de kennisgeving zo laag mogelijk moeten zijn om personen wiens gegevens het betreft te informeren en proportioneel moeten zijn aan de impact. Het is ICT~Office niet duidelijk of de huidige omschrijving toelaat dat een algemene melding wordt gemaakt aan het publiek.

Artikel 34a lid 6 versus artikel 34a lid 1
In artikel 34a lid 6 wordt een uitzondering gemaakt voor het melden aan de betrokkene indien er (naar oordeel van de het Cbp) gepaste technische beschermingsmaatregelen zijn genomen. Indien er echter sprake is van beschermingsmaatregelen zal ook geen sprake zijn een aanmerkelijk risico op verwerking van gegevens waaraan nadelige gevolgen zijn verbonden voor de persoonlijke levenssfeer van de betrokkene (lid 1). Dat impliceert dat er geen gevallen mogelijk zijn waaraan wel aan het Cbp gemeld moet worden, maar de betrokkene niet geïnformeerd hoeft te worden.

Artikel 34a, lid 6
De betrokkene dient door de verantwoordelijke onverwijld te worden ingelicht, terwijl naar aanleiding van het oordeel van de toezichthouder bepaald moet worden of maatregelen voldoende waren (lid 6). Daar de verantwoordelijke volgens het wetsvoorstel een melding onverwijld moet gebeuren, mag daaruit worden afgeleid dat de toezichthouder onverwijld laat weten of maatregelen voldoende waren? ICT~Office herhaalt het voorstel om in lid 2 'onverwijld' te vervangen in 'zo spoedig als redelijkerwijs mogelijk'.

Lid 6 spreekt van 'gepaste technische beschermingsmaatregelen' naar oordeel van het Cbp. ICT~Office stelt voor om een minimale definitie van deze maatregelen te publiceren, zodat het alle verantwoordelijken duidelijk is wat de referentie is voor toetsing.

Artikel II
De Telecommunicatiewet wordt zodanig gewijzigd dat het Cbp de toezichthouder wordt op de meldplicht datalekken voor elektronische communicatieaanbieders. ICT~Office twijfelt sterk over de effectiviteit van deze aanpassing. In de afgelopen periode is veel contact geweest tussen telecommunicatiesector en OPTA, de huidige toezichthouder, om te komen tot pragmatische aanpak in de handhaving van de toekomstige meldplicht datalekken voor aanbieders van elektronische communicatiediensten.

ICT~Office vraagt zich af waarom voor de telecommunicatiesector de markttoezichthouder voor een algemene toezichthouder wordt ingeruild. Gezien de complexiteit binnen de telecommunicatiesector is een specialistische, op deze gevoelige en complexe markt gerichte toezichthouder noodzakelijk, zoals dat ook het geval is bij de banken. Dit kan eventueel in samenwerking met het Cbp, maar niet zonder de specialistische kennis binnen OPTA.

ICT~Office stelt voor om artikel II in zijn geheel uit het wetsvoorstel te schrappen en eerst te oordelen hoe de in de Telecommunicatiewet beoogde situatie in de praktijk zal uitwerken. ICT~Office verwacht dat het beoogde meldpunt voor diverse meldplichten voor deze aanbieders minder lasten oplevert dan het uiteen trekken van de meldingen, met specifieke meldingen voor het CBP en specifieke meldingen voor de markttoezichthouder. Mochten de getroffen voorzieningen geen pragmatische aanpak blijken, dan stelt ICT~Office voor om via een latere wetswijziging de toezichthouder naar het Cbp te veranderen.

Artikel 15 lid 4
In dit artikellid wordt gesproken over een bestuurlijke boete van € 200.000. Dit staat in contrast met artikel 66 lid 2 waarin wordt gesproken over een boete van *ten hoogste* € 200.000. ICT~Office pleit ervoor dat, indien sprake is van sanctionering, boetes in staffels kunnen worden opgelegd. Derhalve verzoekt ICT~Office om 'ten hoogste' ook toe te voegen aan artikel 15 lid 4.

Hoofdkantoor

Bezoekadres
Naritaweg 10
1043 BX Amsterdam

Posladres Postbus 8456, 1005 AL Amsterdam

Posladres
Postbus 8456
1005 AL Amsterdam

T 0900 330 0300
F 020 68 44 541
I www.fnv.nl

Bank
63 50 33 178

De Staatssecretaris van Veiligheid en Justitie
De heer Mr. F. Teeven
Postbus 20301
2500 EH Den Haag

Datum
27 februari 2012
Ons kenmerk
10/003/213
Onderwerp
Consultatie wetsvoorstel camerabeelden en datalekken

Uw kenmerk
5720002/11/6
Telefoonnr.

E-mail

Geachte heer Teeven,

Bij schrijven van 19 december 2011 (kenmerk 5720002/11/6) heeft u de FNV om een reactie gevraagd op het conceptwetsvoorstel over het gebruik van camerabeelden en de meldplicht voor datalekken.

Veiligheid is ook voor de FNV een belangrijk thema. In relatie tot de bescherming van persoonsgegevens verwijzen wij u naar wat wij daarover onder *Beveiliging* hebben opgemerkt in onze brief aan u van 9 november 2010 over de Evaluatie Wet bescherming persoonsgegevens (kenmerk 363/307/12).

Standpunt in het kort
Alvorens meer uitgebreid op de beide onderwerpen van het conceptwetsvoorstel in te gaan, geven wij u hierbij ons standpunt in het kort.
Als organisatie die werknemers en zzp'ers vertegenwoordigt, waardeert de FNV enerzijds het preventieve en repressieve effect van cameratoezicht op de bescherming van personen tegen agressie en geweld en van zaken tegen diefstal en plundering. Anderzijds hecht zij aan de bescherming van werknemers en zzp'ers tegen mogelijke wraakacties en eventuele andere nadelige effecten van het tonen van camerabeelden. Dit leidt ertoe dat de FNV uw redenering en voorstel ten aanzien van een verruiming van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving deels kan volgen, te weten waar het gaat om het direct na een strafbaar feit ter plekke tonen van beelden aan het publiek om een potentieel groot aantal getuigen te bereiken via eigen beeldschermen, billboards e.d. Uiteraard onder de in het wetsvoorstel genoemde condities en

afwegingen van proportionaliteit, subsidiariteit en relatieve zwaarte van de inbreuk op de privacy. Bij de bedoelde condities en afwegingen dient naar het oordeel van de FNV ook uitdrukkelijk rekening te worden gehouden met eventuele op angst voor agressie en geweld gestoelde bezwaren van werknemers van de winkel of zaak die bestolen of beroofd wordt tegen het herkenbaar in beeld worden gebracht. Indien de eigenaar een zelfstandige zonder personeel is, speelt dit uiteraard niet. Die zal eventuele eigen angst voor agressie en geweld laten meewegen in diens wijze van benadering van politie en justitie.
De FNV is echter van mening dat het via internet onder de aandacht van het publiek brengen van camerabeelden van particulieren voorbehouden moet blijven aan openbaar ministerie en politie. Plaatsing op internet kan diep ingrijpen in de persoonlijke levenssfeer van burgers en onherstelbare schade aanrichten. Als politie en justitie camerabeelden van particulieren hebben beoordeeld op bruikbaarheid voor de opsporing en besloten hebben om die beelden niet zelf via internet onder de aandacht van het publiek te brengen, dan moeten (die) particulieren vervolgens geen toestemming krijgen om dat zelf wel te doen.

De FNV hecht sterk aan beveiliging en transparantie. Uw voorstel ten aanzien van de meldplicht van datalekken beoordeelt zij dan ook positief. De FNV verzoekt u bij de verdere uitwerking van dit voorstel al rekening te houden met het Europese conceptvoorstel voor een nieuwe privacyverordening (General Data Protection Regulation), waarin onder meer bepalingen over een meldplicht voor datalekken die zich richt tot elke verantwoordelijke zijn opgenomen (artikelen 28 en 29), inclusief de plicht van elke verantwoordelijke om de betrokkenen over een datalek te informeren.

Gebruik van camerabeelden vervaardigd door particulieren
Criminaliteit in de vorm van overvallen op en diefstal uit winkels of inbraken die gepaard gaan met vernielingen, gevolgd door diefstal bij burgers en bedrijven, maken een diepe indruk op slachtoffers van deze misdrijven. Burgers en bedrijven treffen vaak zelf de nodige beveiligingsmaatregelen tegen deze vormen van criminaliteit. De installatie van beveiligingscamera's is een doelmatige beveiligingsmaatregel. Camerabeelden van strafbare feiten blijken een nuttig hulpmiddel bij de opsporing van deze strafbare feiten. Hoe sneller de beelden bij politie en justitie beschikbaar zijn, hoe groter de kans op een succesvolle opsporing van het strafbare feit en het achterhalen van de verdachten is. Ook blijkt dat het tonen van deze beelden aan het publiek een zinvolle ondersteuning van de opsporing kan zijn.

U merkt op dat het suboptimaal benutten van de mogelijkheden om de beelden te gebruiken leidt tot gevoelens van frustratie en teleurstelling bij de slachtoffers en mogelijk ook tot minder vertrouwen in opsporing en vervolging. Dit kan vervolgens leiden tot het zelfstandig plaatsen van camerabeelden op internet zonder betrokkenheid van politie en justitie. De bedoeling daarvan is reacties van het publiek te verzamelen die kunnen leiden tot de aanhouding van de daders. Terecht merkt u op dat de effecten daarvan onder omstandigheden negatief kunnen zijn. Immers, soms worden personen op ondoordacht verspreide beelden ten onrechte in verband gebracht met strafbare feiten. Dan wordt de privacy van deze burgers geschonden. Ook kunnen de opsporingsbelangen worden doorkruist. Waar het u vooral om gaat is dat de privacywetgeving het gebruik van camerabeelden van particulieren als ondersteuning van de opsporing niet meer, maar

ook niet minder moet reguleren dan strikt noodzakelijk is om een evenwichtige benadering tussen de bescherming van persoonsgegevens en de belangen van opsporing en vervolging van strafbare feiten te bereiken. Vanwege de, wat u noemt, hoog opgelopen maatschappelijke discussie stelt u een met enige urgentie door te voeren herijking van de privacywetgeving op dit onderdeel voor, zodat een wat ruimer gebruik van door particulieren vervaardigde camerabeelden als ondersteuning van de opsporing mogelijk wordt, zonder de belangen van de bescherming van persoonsgegevens te verminderen. Met uw voorstel beoogt u tevens uitvoering te geven aan de door de Tweede Kamer aanvaarde motie van de leden Elissen en Van Toorenburg (Kamerstukken II 2011/12, 33 000 VI, nr. 53). In die motie wordt de regering verzocht om beleid te ontwikkelen zodat burgers zonder angst voor strafrechtelijke vervolging en/ of bestuurlijke beboeting beeldregistraties van overvallers en andere verdachten van misdrijven op internet kunnen zetten of op andere manieren kunnen openbaren mits daarbij aangifte wordt gedaan bij de politie en de beeldregistratie tevens wordt aangeboden aan de politie.

De Wbp staat thans al niet in de weg aan het gebruik van camerabeelden afkomstig van particulieren door politie en openbaar ministerie bij de uitoefening van hun taken. In de Aanwijzing Opsporingsberichtgeving van het College van procureurs-generaal van 16 februari 2009 (Stcrt. 51) zijn richtlijnen gegeven voor de gevallen waarin openbaar ministerie en politie deze beelden gebruiken en op internet en andere manieren onder de aandacht van het publiek brengen. Daarnaast biedt de wet een verantwoordelijke de mogelijkheid camerabeelden waarop te identificeren personen zichtbaar zijn te verwerken ten behoeve van de bescherming van zijn eigen belangen en die van het personeel dat in zijn dienst is. Zo heeft een winkelier de mogelijkheid camerabeelden te maken en te bewaren met het oog op voorkoming en bestrijding van winkeldiefstal door klanten of fraude door het personeel. Gebruik van deze beelden is mogelijk bij het doen van aangifte van diefstal of als bewijsvoering in een ontslagzaak.

Beeldmateriaal dat benut kan worden bij opsporing en vervolging is in ruime mate beschikbaar en burgers en bedrijven zijn bereid dat daartoe beschikbaar te stellen. U noemt in uw wetsvoorstel twee manieren om dat beeldmateriaal efficiënter te benutten. De eerste manier is dat beelden die worden verwerkt door particuliere beveiligingsorganisaties ook buiten de relatie tussen beveiligingsbedrijf en opdrachtgever kunnen worden verwerkt, onder voorwaarden die in het belang van de opsporing en vervolging van strafbare feiten en het belang van de bescherming van persoonsgegevens moeten worden gesteld. De tweede manier is dat particulieren zelf in staat worden gesteld de beelden te verspreiden, eveneens onder voorwaarden die het primaat van de overheid bij de opsporing en vervolging van strafbare feiten veiligstellen en voorwaarden in het belang van de bescherming van persoonsgegevens.
Bij de eerste manier denkt u meer concreet aan het gebruik van beeldschermen die in winkelcentra en in grote afzonderlijke winkels vaak zijn aangebracht om de aandacht van het publiek te zoeken voor hetgeen in de winkel of het winkelcentrum wordt aangeboden. U merkt op dat die beeldschermen in beginsel ook geschikt zijn om de opgenomen beelden van strafbare feiten te tonen aan het bezoekend publiek. Langs die weg kan een potentieel groot aantal mogelijke getuigen worden bereikt. Het tonen van die beelden (via die beeldschermen, nemen wij aan) zou dan gecombineerd moeten worden met een verzoek om melding te maken van relevante feiten bij de beveiligingsorganisatie of aangifte te doen bij de politie. Een dergelijke mogelijkheid

zou alleen geboden behoren te worden wanneer het openbaar ministerie daarvoor toestemming verleent. Daarbij behoren steeds afwegingen van proportionaliteit, subsidiariteit en de relatieve zwaarte van de inbreuk op de privacy te worden betrokken. Een dergelijke voorziening sluit aan bij reeds door de Aanwijzing opsporingsberichtgeving bestreken gevallen waarin met behulp van billboards in de openbare ruimte of in het openbaar vervoer beelden kunnen worden getoond.
Bij de tweede manier denkt u aan meer mogelijkheden voor particulieren om camerabeelden te verwerken zonder de omslachtige en langdurige procedure van het voorafgaand onderzoek door het Cbp. Aangezien het tonen van camerabeelden aan het publiek alleen zinvol kan worden ingezet wanneer dit kort na de opgenomen gebeurtenissen plaatsvindt, heeft het volgen van die procedure meestal niet veel zin. Ook voor deze mogelijkheid geldt dat het primaat van de opsporing van strafbare feiten een overheidstaak blijft. Daarom moet hoe dan ook eerst aangifte worden gedaan van een strafbaar feit en moeten politie en justitie eerst de gelegenheid hebben de beelden te beoordelen op bruikbaarheid voor de opsporing. Politie en openbaar ministerie moeten bovendien eerst zelf de mogelijkheid krijgen de beelden via de eigen middelen te gebruiken. Daarom is onvermijdelijk dat toestemming van het openbaar ministerie nodig is, voordat tot verdere verspreiding via private middelen wordt overgegaan. Aan die toestemming moeten voorwaarden verbonden zijn. Die kunnen betrekking hebben op de wijze van openbaarmaking, de duur van de openbaarmaking en de zorg voor de verwijdering van de beelden.
U besluit uw toelichting met de conclusie dat zolang burgers en bedrijven zich bij het zelf op internet plaatsen van beelden bewegen binnen de voorwaarden die op grond van dit wetsvoorstel worden gesteld – en die bij algemene maatregel van bestuur nader worden ingevuld – die vorm van gegevensverwerking rechtmatig is en er dus niet hoeft te worden gevreesd voor enige vorm van sanctionering. Worden die grenzen overschreden, dan ligt dit natuurlijk anders.

De FNV kan uw redenering en voorstel volgen waar het gaat om het direct na een strafbaar feit ter plekke tonen van beelden aan het publiek om een potentieel groot aantal getuigen te bereiken via eigen beeldschermen, billboards e.d. Uiteraard onder de in het wetsvoorstel genoemde condities en afwegingen van proportionaliteit, subsidiariteit en relatieve zwaarte van de inbreuk op de privacy. Bij de bedoelde condities en afwegingen dient naar het oordeel van de FNV ook uitdrukkelijk rekening te worden gehouden met eventuele op angst voor agressie en geweld gestoelde bezwaren van werknemers van de winkel of zaak die bestolen of beroofd wordt tegen het herkenbaar in beeld worden gebracht. Indien de eigenaar een zelfstandige zonder personeel is, speelt dit uiteraard niet. Die zal eventuele eigen angst voor agressie en geweld laten meewegen in diens wijze van benadering van politie en justitie.

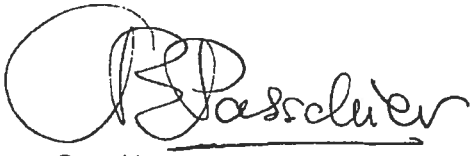
De FNV is echter van mening dat het via internet onder de aandacht van het publiek brengen van camerabeelden van particulieren voorbehouden moet blijven aan openbaar ministerie en politie. Plaatsing op internet kan diep ingrijpen in de persoonlijke levenssfeer van burgers en onherstelbare schade aanrichten. Als politie en justitie camerabeelden van particulieren hebben beoordeeld op bruikbaarheid voor de opsporing en besloten hebben om die beelden niet zelf via internet onder de aandacht van het publiek te brengen, dan moeten (die) particulieren vervolgens geen toestemming krijgen om dat zelf wel te doen. U noemt in uw wetsvoorstel geen overtuigende argumenten voor een ander oordeel.

Meldplicht datalekken

Naar aanleiding van een groot aantal incidenten waarbij door een inbreuk op de beveiliging van onder meer websites persoonsgegevens vrijkwamen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, wordt in het wetsvoorstel een meldplicht voor dergelijke inbreuken ingevoerd. Als niet aan deze meldplicht wordt voldaan zal het Cbp bevoegd zijn een bestuurlijke boete op te leggen van ten hoogste € 200.000,=.
Doel van deze meldplicht is het bevestigen en waar nodig herstellen van het vertrouwen dat de desbetreffende instelling of het desbetreffende bedrijf van het publiek, de klanten, de markt, de overheid en de toezichthouders daarin heeft. Transparantie over de aard van het datalek, de vermoedelijke omvang ervan en de aard van de mogelijke schade, de inspanningen die gepleegd worden om de schade te herstellen en raadgevingen aan publiek en klanten om zichzelf zo goed mogelijk in staat te stellen de consequenties voor de eigen belangen te overzien zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen. Dat vertrouwen wordt ondersteund doordat onafhankelijke toezichthouders in staat worden gesteld om zo nodig te interveniëren

In de uitwerking van de door u beoogde nieuwe voorziening in de Wbp behandelt u onder meer de verhouding tot het geldend Europees recht en merkt u op dat voor een meldplicht voor datalekken die zich richt tot elke verantwoordelijke geen Europeesrechtelijke grondslag bestaat. In uw reactie op onze brief van 19 december (uw brief van 3 december 2010, kenmerk 5677562/10/6 schrijft u onder meer dat u die brief betrekt bij de verdere beleidsvorming die zal plaatsvinden naar aanleiding van de mededeling van de Europese Commissie "Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie" van 4 november 2010, COM (2010) 609. Die mededeling heeft inmiddels geleid tot een conceptvoorstel voor een nieuwe privacyverordening (General Data Protection Regulation), waarin voor het eerst wel bepalingen over een meldplicht voor datalekken die zich richt tot elke verantwoordelijke zijn opgenomen (artikelen 28 en 29). De FNV verzoekt u bij de verdere uitwerking van de meldplicht over datalekken al rekening te houden met het bedoelde Europese conceptvoorstel, dat overigens deels kan dienen als ondersteuning van uw eigen voorstel en waarin ook de plicht van elke verantwoordelijke om de betrokkenen over een datalek te informeren wordt geregeld.

Hoogachtend,



Catelene Passchier,
Federatiebestuurder FNV

SV&J / Sg / DW

NEDERLANDSE ORDE VAN ADVOCATEN

Ministerie van Justitie
DBOB/DIV/OAB/DW
Dossier W1048.7/1074404
Datum 02 MAART 2012
Nummer 12/5726619
Ambt

Ministerie van Veiligheid en Justitie
T.a.v. de Staatssecretaris van Veiligheid en Justitie,
de heer mr. F. Teeven
Postbus 20301
2500 EH Den Haag

3/3

Den Haag, 1 maart 2012
Doorkiesnummer:
Faxnummer:
E-mail:

not 7/3 ond

Betreft: wijziging Wet bescherming persoonsgegevens (gebruik camerabeelden en meldplicht datalekken)

Zeer geachte heer Teeven,

Onlangs heeft u de Nederlandse Orde van Advocaten verzocht te adviseren over de hierboven genoemde wijziging van de Wet bescherming persoonsgegevens.

De Algemene Raad heeft de wijziging voorgelegd aan zijn Adviescommissie Strafrecht die bijgaand advies heeft uitgebracht. De Algemene Raad sluit zich aan bij de overwegingen van de Adviescommissie en verzoekt u deze bij de verdere voorbereiding van de wijziging te betrekken.

Met de meeste hoogachting,
namens de Algemene Raad,

b.a.

mw. mr. R.G. van den Berg
algemeen secretaris

Bijlage

Bezoekadres
Neuhuyskade 94
2596 XM Den Haag
Tel 070 - 335 35 35
Fax 070 - 335 35 31

Postadres
Postbus 30851
2500 GW Den Haag

www.advocatenorde.nl

Preadvies
van de
Adviescommissie Strafrecht
inzake
consultatievoorstel gebruik camerabeelden en meldplicht datalekken

Het wetsvoorstel beoogt twee doelen te bereiken, te weten:

- het op ruimere schaal kunnen inzetten van beelden van "private" beveiligingscamera's om de opsporing van strafbare feiten te ondersteunen ("verruimd gebruik private camerabeelden");

- een verplichting van bedrijven en overheden om lekken in de beveiliging van hun geautomatiseerde verwerking van persoonsgegevens te melden aan het College bescherming persoonsgegevens ("meldplicht datalekken").

Het wetvoorstel leidt niet tot nieuwe strafbaarstellingen van gedragingen. Overtredingen van de nieuwe regels kunnen wel met een bestuurlijke boete worden gesanctioneerd. De Adviescommissie Strafrecht (ACS) ziet toch reden om kort te reageren.

Samenvatting commentaar

- Het wegvallen van enige voorafgaande controle door het College bescherming persoonsgegevens (Cbp) op verwerking van strafrechtelijke gegevens ten behoeve van derden wordt naar de mening van ACS onvoldoende gecompenseerd, waardoor in de te maken afweging de privacybelangen van betrokkene onvoldoende beschermd zijn.

- Het wetsvoorstel noemt onvoldoende redenen waarom datalekken bij verwerkingen die zijn onderworpen aan specifieke wetgeving zoals Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens van de meldplicht datalekken zou moeten worden uitgezonderd.

Verruimd gebruik private camerabeelden: inleiding

Onder "verwerking van persoonsgegevens" verstaat artikel 1 sub b Wet bescherming persoonsgegevens (Wbp) "*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*".

De "*verantwoordelijke*" is "*de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*" (artikel 1 sub d Wbp).

De Wbp regelt vervolgens dat persoonsgegevens alleen op behoorlijke en zorgvuldige wijze worden verwerkt en slechts met het oog op bepaalde gerechtvaardigde doeleinden worden verzameld (artikel 6 respectievelijk 7 Wbp).

Artikel 8 Wbp beperkt de mogelijkheden tot verwerking van persoonsgegevens tot die gevallen waarin:

- de betrokkene ondubbelzinnige toestemming heeft verleend;
- gegevensverwerking noodzakelijk is voor een bepaald in artikel 8 genoemd doel.

Artikel 16 Wbp verbiedt de verwerking van strafrechtelijke persoonsgegevens, waaronder onder meer vallen beelden van personen die mogelijk verdachte zijn van een strafbaar feit.

Dit verbod tot verwerking van strafrechtelijke persoonsgegevens is onder de huidige wet, onder meer, niet van toepassing indien die gegevens ten behoeve van *derden* worden verwerkt en "*passende en specifieke waarborgen zijn getroffen **en** de procedure is gevolgd als bedoeld in artikel 31 Wbp*" (artikel 22 lid 4 sub c Wbp).

De hier bedoelde procedure betreft een onderzoek door het Cbp aan wie zo'n voorgenomen verwerking moet worden gemeld. Indien de verantwoordelijke de strafrechtelijke gegevens wil verwerken ten behoeve van derden, dan stelt het Cbp eerst een onderzoek in.

Volgens de memorie van toelichting (MvT) neemt dit Cbp-onderzoek teveel tijd in beslag. Hierdoor kunnen voor de opsporing bruikbare gegevens (bijvoorbeeld en met name beelden van door burgers en bedrijven zelf in hun ruimten opgehangen beveiligingscamera's) minder snel bij politie en justitie beschikbaar zijn, zodat ook de kans op een succesvolle opsporing minder zou worden. Dit zou, aldus nog steeds de MvT, tot frustratie leiden bij de burgers die ten gevolge daarvan zouden overgaan tot het zelfstandig plaatsen van camerabeelden op internet zonder betrokkenheid van politie en justitie.

Voorgestelde wijziging

Persoonsgegevens in het algemeen en strafrechtelijke persoonsgegevens zijn voor iedere burger zeer private en gevoelige gegevens, die verregaande bescherming verdienen. Vooraleer iemand dergelijke gegevens zonder toestemming van betrokkene aan derden, waaronder politie en justitie, mag verschaffen, moet - terecht - niet alleen aan gepaste waarborgen zijn voldaan, maar ook dient de in bescherming van persoonsgegevens gespecialiseerde toezichthouder te hebben onderzocht of zo'n gebruik gerechtvaardigd is.

Het wetsvoorstel vervangt het woordje "en" in artikel 21 lid 4 sub c Wbp door "of". Voor verwerking ten behoeve van derden is daarom een voorafgaand onderzoek door het Cbp niet meer nodig. De gespecialiseerde toezichthouder die als geen ander kan beoordelen of

de belangen van verwerking ten behoeve van derden zwaarder wegen dan de privacybelangen van betrokkenen zal dus niet meer betrokken worden.

De overgebleven voorwaarde (het treffen van *passende en specifieke waarborgen*) wordt in het voorstel ingevuld door een uit te vaardigen AMvB. De inhoud daarvan zal grotendeels overeenstemmen met de huidige Aanwijzing Opsporingsberichtgeving van het Openbaar Ministerie (d.d. 16 februari 2009). Het wegvallen van controle door het Cbp acht de ACS een te grote stap, zeker nu de passende en specifieke waarborgen niet in de wet worden vastgelegd en uitsluitend nog worden beoordeeld door het Openbaar Ministerie. De vraag rijst of dan nog wel voldoende naar de *specifieke* belangen van privacy wordt gekeken. Juist om te voorkomen dat opsporingsbelangen, al dan niet bewust, te snel de overhand krijgen is tegenwicht van het Cbp waardevol. Overwogen zou kunnen worden de onderzoekprocedure bij het Cbp te verkorten. Het wetsvoorstel meldt overigens niet of deze mogelijkheid is onderzocht en hoe "lang" die procedure in de regel duurt.

Melding datalekken

Met betrekking tot dit onderdeel van het wetsvoorstel volstaat de ACS met de volgende opmerking.

Ingevolge artikel 13 Wbp is iedere verantwoordelijke gehouden de nodige beveiligingsmaatregelen te treffen teneinde te voorkomen dat persoonsgegevens worden gelekt. Volgens het voorstel wordt iedere verantwoordelijke verplicht melding te doen (bij het Cbp) van elke inbreuk op die *maatregelen waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke sfeer van de betrokkene zijn verbonden.*

Dit geldt voor *iedere* verantwoordelijke: natuurlijk persoon of rechtspersoon, private persoon of overheid, behalve als het gaat om verwerkingen die zijn onderworpen aan specifieke wetgeving, zoals de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens. (Mogelijke) datalekken bij verwerkers als politie en justitie behoeven dus niet te worden gemeld. Waarom eigenlijk niet? Juist bij deze instanties gaat het om uiterst gevoelige gegevens.

Amsterdam, 23 februari 2012

Adviescommissie Strafrecht
Mr. R. van der Hoeven, voorzitter,
namens deze, mr. R. Croes-Hoogendoorn, secretaris