

AAN De Minister van Justitie

DATUM 30 september 2010

ONS KENMERK z2010-00949

CONTACTPERSOON

070-8888500

UW BRIEF VAN

UW KENMERK

ONDERWERP Advies betreffende het conceptwetsvoorstel
versterking bestrijding computercriminaliteit

U heeft het College bescherming persoonsgegevens (CBP) gevraagd, ingevolge artikel 51, tweede lid, Wet bescherming persoonsgegevens (Wbp), te adviseren over het over het conceptwetsvoorstel en de bijbehorende memorie van toelichting versterking bestrijding computercriminaliteit.

Het conceptwetsvoorstel bevat de volgende onderdelen:

- a) Opneming in het Wetboek van Strafvordering (Sv) van een zelfstandige regeling van de bevoegdheid van de officier van justitie te vorderen, gegevens op het internet ontoegankelijk te maken. Dit onderdeel is een herziening van artikel 54 a van het Wetboek van Strafrecht (Sr).
- b) Strafbbaarstelling van het wederrechtelijk overnemen van gegevens en het beschikken over of bekend maken van wederrechtelijk overgenomen gegevens: strafbaarstelling van "heling" van computergegevens.
- c) Verruiming van de strafbepalingen betreffende het afluisteren, aftappen of opnemen van vertrouwelijke communicatie.

Hiermee voldoe ik aan uw verzoek.

Achtergrond

Op 1 maart 1993 is de Wet Computercriminaliteit in werking getreden. In deze wet zijn in Sv bevoegdheden tot onderzoek naar geautomatiseerde werk en in Sr specifieke strafbepalingen rond de wederrechtelijke toegang tot computers en het misbruik van gegevens toegevoegd. Met de Wet Computercriminaliteit II (per 1 september 2006 in werking getreden) zijn in verband met de technologische ontwikkelingen Sv en Sr aangepast. De Registratiekamer, de rechtsvoorganger van het CBP, heeft over het wetsvoorstel Computercriminaliteit II in 1998 een advies uitgebracht (*advies van 9 maart 1998, 98.A.089.01*).

De voortschrijdende ontwikkelingen op het terrein van de informatie- en communicatietechnologie, waardoor het overnemen en verspreiden daarvan over het internet steeds eenvoudiger wordt, maken het noodzakelijk dat ter bescherming van de persoonlijke levenssfeer en de vertrouwelijke communicatie, computergegevens een ruimere strafrechtelijke bescherming bieden (MvT, p. 2).

Het advies, bespreking voorgestelde wijzigingen

a) ***De bevoegdheid voor de officier van justitie te vorderen dat gegevens ontoegankelijk worden gemaakt: artikelen 125p en 125 q Sv.***

Deze bevoegdheid is van belang in die gevallen waarin de aanbieder van een communicatiedienst of degene die de beschikkingsmacht heeft over een geautomatiseerd werk, niet bereid is op basis van de gedragscode "Notice-And-Take-Down" de gegevens ontoegankelijk te maken en een vordering van de officier van justitie nodig is om het strafbare feit te beëindigen of om nieuwe strafbare feiten te voorkomen.

De gedragscode "Notice-And-Take-Down" is van toepassing op tussenpersonen die in Nederland een openbare (telecommunicatie-) dienst op internet leveren en bevat een procedure voor het omgaan met meldingen van onrechtmatige en strafbare inhoud op internet. Op basis van deze gedragscode moet de tussenpersoon, na een melding, ervoor zorgen dat, indien er naar het oordeel van de tussenpersoon sprake is van onmiskenbaar onrechtmatige of strafbare inhoud, die inhoud onverwijld door de tussenpersoon verwijderd wordt. Indien aan de melding geen gehoor wordt gegeven kan de melder overgaan tot het doen van aangifte of de rechter betrekken. Ook de politie kan verzoeken om verwijdering doen als het gaat om kinderporno die in Nederland wordt "gehost".

Indien de gedragscode niet afdoende blijkt om verwijdering van de gegevens te realiseren, kan de officier van justitie gebruik maken van zijn bevoegdheid in het voorgestelde artikel 125p Sv. In dit artikel wordt de vorderingsbevoegdheid van de officier van justitie geregeld en de voorwaarden waaraan deze vordering dient te voldoen. Op grond van het voorgestelde artikel 125q Sv kan de officier van justitie in de vordering als bedoeld in artikel 125p Sv een dwangsom opleggen aan degene tot wie de vordering is gericht.

Rechtsbescherming

Artikel 125p Sv voorziet alleen in het ontoegankelijk maken van de gegevens. Over de vraag of de gegevens vervolgens ook moeten worden vernietigd, beslist de rechter. Op grond van artikel 552a Sv kunnen belanghebbenden zich bij de raadkamer van de rechtbank schriftelijk beklagen over de vordering tot het ontoegankelijk maken van gegevens. Het beklag strekt zich mede uit over de mogelijk opgelegde dwangsom als bedoeld in artikel 125q Sv. Door deze voorziening is het niet meer noodzakelijk, zoals dat nu is bepaald in artikel 54 a Sr, dat er een voorafgaande schriftelijke machtiging van de rechter-commissaris noodzakelijk is (MvT, p. 5).

Oordeel

De voorgestelde wijziging geeft geen aanleiding tot opmerkingen, de geboden rechtsbescherming lijkt adequaat.

b) ***Wederrechtelijke overname van gegevens en het beschikken over en bekend maken van wederrechtelijk opgenomen gegevens: artikel 54a Sr.***

Door de technische ontwikkelingen wordt het steeds eenvoudiger om gegevens uit computers over te nemen en vervolgens op het internet te zetten. Vertrouwelijke gegevens kunnen daardoor razendsnel worden verspreid en worden voor grote groepen mensen toegankelijk. Verwijdering van het internet is vervolgens niet eenvoudig. Vooral met het oog op de persoonlijke levenssfeer dient strafrechtelijk te kunnen worden opgetreden. In de voorgestelde regeling zijn twee nieuwe strafbaarstellingen voorzien:

1. Het wederrechtelijk overnemen van gegevens uit een computer, in die gevallen waarin gegevens gekopieerd zijn en de rechthebbende dus de beschikking houdt over de gegevens. De rechthebbende kan geen invloed uitoefenen over het gebruik van deze gegevens en kan daardoor benadeeld worden.
2. Strafrechtelijke aansprakelijkheid van degene die over dergelijke gegevens beschikt of deze bekend maakt: "heling". Strafbaarstelling is mogelijk ook indien niet kan worden aangetoond dat de persoon die deze gegevens bekend maakt ook degene is die deze gegevens heeft overgenomen.

De toevoeging van de term 'overnemen' maakt strafbaarstelling mogelijk van personen die rechtmatige toegang hebben tot bepaalde gegevens, maar deze zonder daartoe gerechtigd te zijn deze voor zichzelf of anderen overneemt. Omdat de rechthebbende de beschikking over de gegevens houdt is vervolging op grond van 321 Sr (verduistering) niet mogelijk. Met het gebruik van de term 'overnemen' wordt tot uitdrukking gebracht dat het niet vereist is dat gegevens buiten de beschikkingsmacht van de rechthebbende (zoals bij verduistering) worden gebracht. Heling van dergelijke gegevens wordt via artikel 139e Sr strafbaar gesteld.

Oordeel

Deze strafbaarstelling brengt (wederom) aan het licht dat het treffen van adequate beveiligingmaatregelen (zowel in organisatorische als in technische zin) onontbeerlijk is en moet de verantwoordelijken vooral niet ontslaan van zijn verplichtingen zoals die uit artikel 13 van de Wbp voortvloeien.

c) Afluisteren, aftappen, opnemen of overnemen van gegevens: artikelen 139a, 139b, 139 c en 139e Sr.

Het betreft hier verruiming van de strafbaarstellingen, dat wil zeggen dat de voorwaarden dat de dader zelf geen gespreksdeelnemer is dan wel dat de gegevens niet bestemd zijn voor degene die gegevens opneemt of aftapt komen te vervallen.

In de strafbaarstelling is de volgende situatie uitgezonderd: "... maar ook in de gevallen waarin het zonder toestemming/medeweten van een van de deelnemers opnemen van de communicatie civielrechtelijk niet onrechtmatig is, bijvoorbeeld in het uitzonderlijke geval dit noodzakelijk is om misstanden aan de kaak te stellen en dit belang zwaarder weegt dan de belangen die zijn gemoeid met de bescherming van de persoonlijke levenssfeer van de deelnemers aan de communicatie" (MvT, p.12).

Oordeel

Op pagina 18 van de MvT wordt opgemerkt dat het wederrechtelijke karakter, onder verwijzing naar paragraaf 4 van de MvT (p. 12), aan het opnemen of aftappen van die communicatie kan komen te ontvallen. In de delictomschrijving (van artikel 139c Sr) is die uitzonderingsgrond niet opgenomen. Maar wat betekent "civielrechtelijk niet onrechtmatig", is dat naar eigen goeddunken vast te stellen door degene die deze gesprekken opneemt en/of aftapt of is dat aan de civiele rechter om te beoordelen? Indachtig de persoonlijke levenssfeer van degenen die hierbij zijn betrokkenen acht het CBP een nadere toelichting op dit punt in de MvT noodzakelijk.

Het CBP adviseert aan het vorenstaande passende aandacht te schenken op te nemen. Indien er naar aanleiding van dit advies behoefte is aan een nadere toelichting dan ben ik daartoe graag bereid.

DATUM 30 september 2010
ONS KENMERK z2010-00949

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

Mw. mr. dr. J. Beuving
Lid van het College