

## Ministerie van Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer  
der Staten-Generaal  
Postbus 20018  
2500 EA DEN HAAG

**Directoraat-Generaal  
Preventie, Jeugd en  
Sancties**

Directie Sanctie- en  
Preventiebeleid  
Afdeling sanctie- en  
reclasseringsbeleid

Schedeldoekshaven 100  
2511 EX Den Haag  
Postbus 20301  
2500 EH Den Haag  
[www.justitie.nl](http://www.justitie.nl)

**Ons kenmerk**  
5606234/09/DSP

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

Datum 1 juli 2009

Onderwerp **Antwoorden op vragen van het lid Gerkens (SP) over het  
verbergen van kinderporno op computers en het toezicht  
daarop**

Hierbij doe ik u mede namens de Minister van Justitie de antwoorden toekomen op de vragen van het lid Gerkens (SP) over het verbergen van kinderporno op computers en het toezicht daarop (ingezonden op 1 april 2009, met kenmerk 2009Z06067).

De Staatssecretaris van Justitie,

**2009Z06067**

**Vragen van het lid Gerkens (SP) aan de staatssecretaris van Justitie over het verbergen van kinderporno op computers en het toezicht daarop (ingezonden 1 april 2009)**

---

**Directoraat-Generaal  
Preventie, Jeugd en  
Sancties**  
Directie Sanctie- en  
Preventiebeleid  
Afdeling sanctie- en  
reclasseringsbeleid

**Datum**  
1 juli 2009

**Ons kenmerk**  
5606234/09/DSP

**Vraag 1**

**Wat is uw reactie op de conclusie in de uitzending van Undercover Nederland dat politie en justitie technisch niet in staat zijn versleutelde gegevens, zoals kinderpornografische afbeeldingen, te ontsleutelen?**

**Antwoord 1**

Computerprogramma's om gegevens van de harde schijf te wissen, surfsporen te verwijderen of bestanden veilig op te slaan bestaan reeds enige jaren. Een klein deel van de kinderpornoverdachten gebruikt deze tools. Mede daarom gaan politie en Openbaar Ministerie de strafrechtelijke aanpak van kinderpornografie aanzienlijk versterken. Het College van procureurs-generaal heeft inmiddels een landelijk coördinerend officier kinderpornografie aangesteld. Deze landelijke coördinator moet voorzien in zowel een kwalitatieve als kwantitatieve versterking van de opsporing en vervolging van kinderpornografie.

Bestrijding van cybercrime vraagt om een andere wijze van werken, met andere methoden en technieken. Verdere kennis en vaardigheden over de technische en strafvorderlijke aspecten van cybercrime is nodig om in voorkomende gevallen te kunnen optreden. De komende tijd zal daarom verder worden geïnvesteerd in technologische ontwikkeling ter bestrijding van het hebben en verspreiden van kinderpornografische afbeeldingen. Onderdeel hiervan is het kunnen opsporen van versleutelde gegevens, zoals kinderpornografische afbeeldingen.

**Vraag 2**

**Waaruit bestaat op dit moment het toezicht van de reclassering op mensen die zijn veroordeeld voor het in bezit hebben van kinderpornografische afbeeldingen? Hoe kan het dat iemand die onder reclasseringstoezicht staat vrijelijk het internet op kan zonder dat gecontroleerd wordt welke websites bezocht worden en wat er gedownload wordt?**

**Antwoord 2**

Het reclasseringstoezicht wordt afgestemd op het risico van overtreding van de voorwaarden. Zedendelinquenten waarvoor een strikte controle noodzakelijk is, worden doorgaans intensief gevolgd, zodat signalen van terugval en dreigende recidive tijdig worden opgemerkt en direct kan worden ingegrepen. De meest intensieve vorm van toezicht bestaat uit onverwachte controle-bezoeken, een hoge gespreksfrequentie met de justitiabele, veel controle van behandel- en zorguitvoerders en de inzet van elektronische controlemiddelen. In het kader van de begeleiding van en het toezicht op de delinquent wordt ook veelal intensief contact onderhouden met het sociale netwerk, behandelaars, politie en eventueel werkgevers.

Volgens de wet is het Openbaar Ministerie verantwoordelijk voor het toezicht op de naleving van de voorwaarden. In de praktijk kan de rechter de reclassering opdracht geven de veroordeelde hulp en steun te verlenen bij de naleving van de voorwaarden. Dit laatste wordt reclasseringstoezicht genoemd. Indien er aanwijzingen zijn dat betrokkene de voorwaarden overtreedt, wordt melding gemaakt bij de officier van Justitie. Deze is bevoegd tot nader onderzoek door bijvoorbeeld de technische recherche dan wel tot het direct vorderen van de vervangende hechtenis. Afhankelijk van de beslissing van de rechter wordt betrokkene vervolgens ingesloten. Deze aanwijzingen kunnen bestaan uit signalen vanuit het sociale netwerk en behandelaars. Buiten de feitelijke toezichtsmomenten blijft overigens altijd de mogelijkheid bestaan dat iemand die onder reclasseringstoezicht staat vrijelijk het internet op gaat. Daarbij valt te denken aan het internetgebruik op een andere locatie dan thuis, zoals een bibliotheek.

**Directoraat-Generaal  
Preventie, Jeugd en  
Sancties**

Directie Sanctie- en  
Preventiebeleid  
Afdeling sanctie- en  
reclasseringsbeleid

**Datum**  
1 juli 2009

**Ons kenmerk**  
5606234/09/DSP

**Vraag 3**

**Bent u ermee bekend dat het technisch gezien goed mogelijk is het internetgedrag van mensen te monitoren en dat daar al jarenlang software voor bestaat?**

**Antwoord 3**

Ja, er zijn diverse mogelijkheden het internetgedrag van mensen te monitoren. Deze softwareprogramma's zijn echter niet altijd volledig betrouwbaar en richten zich bovendien op één computer, terwijl soms ook vanuit meerdere pc's het internet wordt opgegaan.

**Vraag 4**

**Bent u ervan op de hoogte dat deze software bij de reclassering bekend is? Waarom wordt deze software niet gebruikt?**

**Antwoord 4**

Op dit moment worden door de reclasseringsorganisaties de mogelijkheden verkend om het toezicht te laten ondersteunen door forensische softwareprogramma's. De resultaten van deze verkenning zullen aan het einde van dit jaar gereed zijn. De reclasseringsorganisaties doen dit in overleg met de KLPD. Indien er nu aanwijzingen zijn dat betrokkene de voorwaarden overtreedt, wordt melding gemaakt bij het OM. Deze is bevoegd tot nader onderzoek van de computer door bijvoorbeeld de technische recherche.

**Vraag 5**

**Welke keuringsprocedure moet dergelijke software doorgaan? Bent u bereid deze software te keuren? Zo nee, waarom niet?**

**Antwoord 5**

De door de reclasseringsorganisaties te gebruiken softwareprogramma's moeten voldoen aan eisen van betrouwbaarheid en validiteit. Dit is van belang met het oog op een rechtmatige bewijsvoering van overtreding van de voorwaarden.

**Vraag 6**

**Wat heeft u tot dusver gedaan met de kennis van het bestaan van deze software? Vindt u het wenselijk om het internetgedrag van mensen die met behulp van hun computer misdrijven hebben gepleegd, zoals ook**

**andere vormen van cybercrime, gedurende het reclasseringstoezicht in de gaten te houden? Zo nee, waarom niet?**

**Antwoord 6**

Ik verwijs hiervoor naar het antwoord op vraag 4.

**Directoraat-Generaal  
Preventie, Jeugd en  
Sancties**

Directie Sanctie- en  
Preventiebeleid  
Afdeling sanctie- en  
reclasseringsbeleid

**Datum**  
1 juli 2009

**Ons kenmerk**  
5606234/09/DSP