**Henk J. Schanssema**

**Zelfstandig Adviseur Technologie en Recht**

**Onderwerp**
Consultatiedocument wetsvoorstel versterking bestrijding computercriminaliteit

**Datum**
28 september 2010

## 1. Verwijderen gegevens internet

### 1.1. Inleiding

Op 15 september 2010 is door o.a. Bits Of Freedom[1] een "brandbrief" gezonden met betrekking tot dit onderwerp. Met de inhoud ervan wordt uitdrukkelijk ingestemd.

### 1.2. Niet de provider, maar de overtreder aanpakken

Het wetsvoorstel lijkt vooral gericht te zijn op comfort voor het OM, echter ten koste van fundamentele, rechtsstatelijke beginselen. De trias politica wordt kreupel gemaakt en daarnaast hoeft het OM weinig te doen om "omstreden" informatie ontoegankelijk te maken. Het leidt echter tot een foute prikkel, want het *werkelijke probleem wordt niet bestreden* en het OM zou zelfs achterover kunnen gaan leunen.

### 1.3. Moet de provider toezicht houden en voor rechter gaan spelen?

Het wetsvoorstel lijkt de internet provider ("aanbieder van een communicatiedienst") te verplichten toezicht te houden op al hetgeen via zijn dienst wordt aangeboden, want art. 54 Sr (ontwerp) leent zich voor die uitleg, waarbij tegelijkertijd van de provider wordt gevergd, dat hij vaststelt wat er eventueel strafbaar is. De provider wordt met straf bedreigd zodra er eventueel sprake is van een straf*baar* feit, echter hoe kan de provider dat zelf objectief vaststellen?

### 1.4. Kleine providers lopen grote risico's

Er zijn vele internet providers, in ongeveer evenveel hoedanigheden. Vooral kleinere providers, waaronder vele eenmansbedrijven, zullen niet steeds redelijkerwijs in staat zijn om een bevel ex art. 125p Sv (ontwerp) tijdig op te volgen. Een simpel voorbeeld is een vakantieperiode. Zelfs grote providers zijn doorgaans tijdens weekeinden en feestdagen beperkt bereikbaar. Het wetsvoorstel schrijft geen termijnen voor, dus kan het OM bevelen geven, die binnen zeer korte tijd, misschien wel uren, moeten worden opgevolgd.

### 1.5. Verkeerde provider?

Het internet is technisch uitermate gecompliceerd. Lang niet altijd is duidelijk, waar de eventueel strafbare gegevens staan. Talloze aanbieders nemen diensten af van

[1] De betreffende brief is mede ondertekend door een reeks organisaties en vooraanstaande rechtswetenschappers.

bijvoorbeeld grotere providers of datacentra en registreren domeinnamen via derden. Ik acht de kans bijzonder groot, dat aan de verkeerde aanbieder een bevel wordt gegeven, simpelweg omdat zeer waarschijnlijk de deskundigheid bij het OM tekort schiet. Daarbij moet worden bedacht dat eventuele personen die opzettelijk strafbaar materiaal publiceren, veelal trachten de identiteit zoveel mogelijk te verhullen.

In de bijlage is een praktijkvoorbeeld opgenomen waarbij het domein **om.nl** onder de loep werd genomen op een willekeurige dinsdagavond. Resultaat: niemand bereikbaar en een niet bestaand telefoonnummer, dus onjuiste gegevens van het OM zelf!

Een bekend voorbeeld is The Pirate Bay. Ondanks rechterlijke bevelen die de site onbereikbaar moesten maken, draait deze site nog steeds. Het is volstrekt onduidelijk waar de servers staan. Weet het OM dat dan wel?

### 1.6. Dwangsom

Gezien de hiervoor geschetste bezwaren, kan een dwangsom zeer verstrekkende consequenties hebben. Zodra het OM (**en niet de rechter!**) eenmaal oordeelt dat niet is voldaan aan een bevel, kan een dwangsom worden opgelegd die vrijwel onmiddellijk executoir is. Vooral kleinere entiteiten lopen het risico volledig ten onder te gaan indien een forse dwangsom wordt opgelegd, die achteraf kan blijken *onterecht* te zijn geweest. Maar de betrokken aanbieder is inmiddels misschien wel failliet!

## 2. Overnemen niet-openbare gegevens

### 2.1. Inleiding

In algemene zin acht ik het voorstel onwenselijk. Er is voldoende civiel recht gevormd waarmee een benadeelde de "dader" kan aanspreken. Wat voegt een strafdreiging toe? Een beoordeling vanuit het perspectief van het resultaat is naar mijn mening helder: de vlag dekt de lading niet, of er worden andere doelen nagestreefd, dan thans gepresenteerd.

### 2.2. Gegevensbeveiliging "by design"

Zo er al preventief effect gesorteerd moet worden (want dat zou in theorie het effect van strafdreiging zijn), acht ik gegevensbeveiliging "by design" veel effectiever. Als ICT-deskundige kan ik alleen maar vaststellen dat beveiliging in de praktijk vaak een waarlijk "tranendal" is. Bits Of Freedom houdt terecht datalekken bij. Elk datalek bewijst dat preventie sterk tekort schiet. Het is het topje van de ijsberg, want veel incidenten worden niet bekend, omdat het schadelijk kan zijn voor het imago van de betrokken organisatie.

Een simpele vergelijking met een slot op de voordeur: er zal een zekere relatie zijn tussen strafdreiging en de kans op inbraak, maar ook zal de kwaliteit van (onder meer) het hang- en sluitwerk afhankelijk zijn van de strafdreiging. Als inbraak niet met straf zou worden

bedreigd, dan zouden huizen veel beter beveiligd zijn en bewoners veel alerter zijn. Ik acht de kans groot dat het voorstel een (meer) lakse houding ten aanzien van de beveiliging van gegevens in de hand werkt en er dus per saldo niets wordt bereikt.

De kwestie met de foto's van mevrouw Thomas illustreert de noodzaak van beveiliging of preventief wissen van gegevens. Het "niet hebben" van gegevens biedt nog altijd de beste en meest eenvoudige waarborgen tegen ongewenste verspreiding.

Indien wordt verondersteld dat het effect nul zal zijn (door de laksere houding, die de kans op datalekken vergroot), dan is het recht op informatie het kind van de rekening en is het totaalresultaat een achteruitgang.

2.3. **Ineffectief en ondoordacht**

Het wetsvoorstel vind ik slecht en ondoordacht. Slecht, omdat bezit niet meteen leidt tot verspreiding. Er dreigt immers pas een probleem, als informatie aan derden wordt doorgegeven. Om het voorbeeld van de foto's van mevrouw Thomas erbij te nemen: het "probleem" is recht evenredig met de mate van verspreiding van de gegevens en daarnaast weegt de mate van inbreuk op het belang van de benadeelde mee.

Tevens speelt het karakter van de informatie een rol, die niet tot uitdrukking komt in het voorstel. Zo is schade door het "uitlekken" van bedrijfsinformatie vaak ernstiger dan in het geval van het "uitlekken" van foto's van een "BN'er". De bedrijfsinformatie hoeft slechts bij een zeer kleine kring van belangstellenden terecht te komen, om schade te verwezenlijken. Bij de fotokwestie is juist de verspreidingsgraad van meer betekenis.

Ondoordacht is het voorstel, omdat het gemakkelijk te omzeilen is. Ik neem een denkbeeldig geval van bedrijfsspionage als voorbeeld. Een technisch bekwame "dief" zal trachten eventuele sporen uit te wissen. Hackers weten bij uitstek hoe dat in de praktijk werkt. Men verhult de identiteit door veelal via (een reeks) gehackte computers te werk te gaan. Het is tevens erg makkelijk om de informatie zodanig te "verplaatsten" dat de wet gatenkaas zal blijken. Stel dat de informatie meteen wordt verplaatst naar een server in een ver land. Wie bezit het dan? Goodbye, ontwerp art. 139e lid a Sr! Als vervolgens de informatie door belanghebbende slechts wordt ingezien, is lid b ook meteen omzeild. Juridisch gezien zijn de feiten misschien wel strafbaar, maar het bewijs krijgt het OM nooit rond (afgezien van een enkel geval waar het dataverkeer misschien was getapt en er dus mogelijk al sprake van een verdenking was).

Met een modern mobieltje is "ouderwetse spionage" reuze makkelijk. Even de foto's uploaden via UMTS, of het heel kleine flashkaartje goed verstoppen, het is zo ontzettend eenvoudig! Het wetsontwerp geeft weinig blijk van technische realiteitszin.

2.4. **Verkeerde bijvangst**
Bits of Freedom wees er al op in de eerdergenoemde brandbrief: soms is het een essentieel maatschappelijk belang, dat niet-openbare gegevens worden geopenbaard.

Ook kan er een privaat belang gediend zijn met het beschikken over gegevens, die wellicht zonder toestemming zijn verkregen. Civiele rechters hebben dagelijks te maken met partijen die een verkeerde voorstelling van zaken geven, wetende dat de wederpartij bewijsproblemen heeft, bijvoorbeeld omdat er mondelinge afspraken zijn gemaakt, die nu eenmaal niet of erg lastig te bewijzen zijn. Zou een partij beschikken over materiaal, dat wellicht als inbreukmakend of wederrechtelijk te beschouwen is, maar waarmee de waarheid gediend is, kan de civiele rechter een afweging maken. Het wetsvoorstel krijgt van mij daarom een "anti-waarheid" predikaat!

2.5. **Downloadverbod?**
Een (misschien wel bedoelde?) nevenwerking is het bewerkstelligen van het door media-uitgevers zo fel begeerde downloadverbod. Want een "kopietje van een MP3'tje" wordt in beginsel strafbaar. Voor de bezitter van legaal verkregen mediabestanden wordt het wetsvoorstel eveneens riskant, want lang niet altijd is eenvoudig vast te stellen of een licentie is verkregen. Waar het voor eigen gebruik opnemen van muziek (bijvoorbeeld van de radio) thans niet als inbreukmakend wordt gezien, kan het wetsvoorstel ongekende beperkingen opleveren.

**2.6. Ontslagservice?**
Interessant is het volgende hypothetische voorbeeld, dat inzichtelijk maakt hoe het wetsvoorstel verstrekkende, onbedoelde neveneffecten kan bewerkstelligen. Een werkgever wil van een werknemer af. De werknemer verricht op verzoek van de werkgever thuiswerk en neemt op een draagbare computer bedrijfsinformatie mee. Vervolgens beticht de werkgever de werknemer van bezit van gegevens, waarvoor geen toestemming is gegeven en doet aangifte. De rest laat zich raden. Het voorbeeld illustreert, hoe onder omstandigheden verdachten kunnen worden "gecreëerd". Hieronder wordt nog uiteengezet, dat facetwederrechtelijkheid zich bij dit wetsvoorstel doet voelen.

2.7. **Omgekeerde wereld**
De conclusie is, dat het wetsvoorstel door malafide personen zal worden omarmd, terwijl de bescherming van maatschappelijke en individuele belangen om zeep wordt geholpen.

## 3. Opnemen privé-gesprekken

3.1. **Inleiding**
Het wetsvoorstel negeert de gerechtvaardigde belangen van burgers, dat vooral gelegen kan zijn in waarheidsvinding, in het geval een malafide partij bijvoorbeeld mondelinge

afspraken niet nakomt. Een inventarisatie van het "probleem" ontbreekt, evenals zicht op de (nadelige) gevolgen van het wetsvoorstel.

3.2. **Vergaren informatie vertegenwoordigt gerechtvaardigd belang**
Soms kan het reuze nuttig zijn om informatie te vergaren, die niet kon worden verkregen als de informant zou weten dat het gesprek zou worden vastgelegd. Uit eigen ervaring weet ondergetekende, dat een liegende partij bij de civiele rechter tot inkeer kan worden gebracht middels een (transcriptie van) een "verhelderend" telefoongesprek. De huidige rechtspraak is, dat de rechter - eenvoudig weergegeven - het belang van inbreuk (op privacy) weegt tegenover het belang van de waarheidsvinding en het laatste kan laten prevaleren.

In de toelichting onder 4 wordt gesteld dat er onder omstandigheden sprake kan zijn van verschoonbare omstandigheden, echter voorziet de tekst van het wetsvoorstel daar niet in. Bovendien is het *vastleggen als zodanig* reeds strafbaar, waardoor dat aan een serieus strafrisico wordt blootgesteld. Eventuele verschoonbare omstandigheden, die daarbij niet op voorhand duidelijk zullen zijn, moeten door de verdachte worden aangetoond, waardoor via de achterdeur de bewijslast wordt omgekeerd.

3.3. **Niet het vastleggen, maar openbaarmaking eventueel strafbaar stellen**
Zolang er met een opname niets wordt gedaan, is er geen enkel recht of belang geschonden. Niet valt in te zien, waarom die fase reeds strafbaar wordt gesteld. Indien een opname openbaar wordt gemaakt, **zonder redelijke noodzaak**, is een strafdreiging eventueel voor te stellen. Ik kan echter niet zien waarom de huidige praktijk niet kan blijven voortbestaan.

## 4. Facetwederrechtelijkheid

4.1. **Civiele toestemming is sleutel**
Het meest verstrekkende bezwaar acht ik de sterk *civielrechtelijke* aard van de eventuele wederrechtelijkheid. Immers gaat het om al dan niet verleende *toestemming* voor het bezit en of gebruik van gegevens. Een bijkomend bezwaar is gelegen in de kans, dat een oorspronkelijk verleende toestemming later wordt ontkend. Ook is denkbaar dat een toestemming achteraf wordt geweigerd. Tevens wordt aandacht gevraagd voor de omstandigheid dat een eerder verleende toestemming wordt ingetrokken of dat de toestemming onder zeker voorwaarden was gegeven. Alleen dit laatste kan al aanleiding zijn tot uitvoerige debatten of eventuele voorwaarden vervuld zijn.

4.2. **Bewijsaspecten**
De rechter zal moeten toetsen of er toestemming is gegeven. Dit lijkt geen gemakkelijke opgave, zeker als toestemming mondeling is gegeven. De aard van de gegevens kan tevens

een rol spelen bij aannamen van de rechter. Immers zal bij zeer vertrouwelijke gegevens minder snel toestemming worden aangenomen. Ik acht ook in dit verband de kans aanwezig dat civiel bewijsrecht "via de achterdeur" het strafrecht binnenkruipt en bovendien doemt de omgekeerde bewijslast op (bewijs van onschuld).

Daarnaast is denkbaar dat bijvoorbeeld een geluidsopname met toestemming is opgenomen, maar dat de wederpartij in een civiele procedure verklaart geen toestemming te hebben gegeven. Kan de toestemming niet worden bewezen, is de opname onbruikbaar (en zelfs eventueel strafbaar). Het wetsvoorstel tast de positie aan van degene, die een legitieme opname wil maken als eventueel bewijs van mondelinge afspraken.

*Henk J. Schanssema (1955)*

*Ondernemer*
*Student rechtswetenschappen*

## Bijlage

Een praktijkcase, 28 september 2010, ca. 21.26 uur. Als testobject dient **www.om.nl.**

De registratiegegevens van het domein **om.nl**:

```
[Querying rwhois.domain-registry.nl]
[rwhois.domain-registry.nl]
Domain name: om.nl
Status:      active

Registrant:
   OPE000236-ASP4A
   openbaar ministerie
   Prins Clauslaan 16, 2595AJ 'S-GRAVENHAGE, Netherlands
   +00.00000000
   gegevens.onbekend@sidn.nl

Administrative contact:
   GOR005978-ASP4A
   F. Gorter
   +31.703399833
   webbureau@om.nl

Registrar:
   ASP4all Hosting B.V.
   Energieweg 8
   1271ED HUIZEN
   Netherlands

Technical contact(s):
   MAA002130-ASP4A
   Afd. Registratie ASP4all
   Energieweg 8, 1271ED Huizen, Netherlands
   +31.0355232626
   registratie@asp4all.nl

Domain nameservers:
   ns1.asp4all.nl       62.112.224.60
   ns2.asp4all.nl       62.112.236.60
   ns3.asp4all.nl       62.112.244.60

Date registered: 1997-03-04

Date of last change: 2010-02-10
```

Ik bel het nummer van het administratieve contact, F. Gorter. 070-3399833 blijkt niet in gebruik te zijn. Dan ASP4all gebeld, 035-5232626. "Wij zijn op *werkdagen* [cursief HJS] geopend van 8 uur 's ochtends tot 8 uur 's avonds".

Niemand bereikbaar dus, inclusief een niet bestaand nummer.

Hoe gaat een "spoedbevel" hier in zijn werk?