Iedereen hoort wel eens van een actie van de politie, waarbij er ergens preventief moet worden gefouilleerd. In het *Wetboek van Strafvordering* was enige jaren geleden fouillering wel aan een aantal strenge regels gebonden. Je mocht niet zo maar iemand gaan fouilleren. Dat gebeurde overigens pas als iemand was aangehouden (gearresteerd) en er voldoende verdenking aanwezig was om tot fouillering over te gaan. Tegenwoordig is dat wel anders geworden. Plotseling worden burgers in een politiefuik opgevangen en zomaar zonder reden binneste buiten gekeerd. En als je de cijfers mag geloven zijn de meesten onschuldig van hun rechten beroofd.

Er is onlangs iemand geweest die zich heeft afgevraagd hoeveel wetten en maatregelen erbij zijn gekomen in de afgelopen jaren die onze privacy aantasten. Columniste *Karin Spaink* heeft dat op haar blog gezet. Die heeft het weer van een zekere *Paul Vogel* die het op zijn beurt als eerste had gepubliceerd. En wat opvalt is dat er in de afgelopen jaren geen middel tot opsporing is onthouden aan de bevoegde opsporingsinstanties**. Een van de meest onthutsende indringingsmethoden vond hij bij politie en justitie. Wie bijvoorbeeld bij zijn of haar Internet Service Provider een account heeft om op het internet te gaan, die weet niet dat dagelijks de NAW-gegevens (Naam, Adres, Woonplaats) en zelfs wachtwoorden worden doorgestuurd naar de justitiële databank het *CIOT* (*Centraal Informatiepunt Opsopring Telecom*). Let wel: bijna geen burger weet daarvan en politie en justitie maken gretig gebruik (of misschien misbruik) van de gedeponeerde data met een opvraag van maar liefst 1.3 miljoen keer in 2005! Via deze databank kan men snel checken wie achter een bepaald nummer schuilgaat, of welk nummer bij welke naam of adres hoort. In een mum van tijd zijn de NAW-gegevens op te vragen zelfs als men al een IP-adres van de computer weet te bemachtigen. En dan het tweede schokkende detail: er zijn 1,3 miljoen entry's in 2005 ongevraagd gevisiteerd door de politie via hun ISP...Waar zijn die absurde hoeveelheden voor nodig?**

Het begint er steeds meer op te lijken dat de Overheid en de Opsporingsinstanties steeds dieper, veelvuldiger en volstrekt ongevraagd het privédomein van de burger binnen kan treden, maar dit gebeurt dan zonder dat die burger daar iets tegenover kan stellen. Naar ons idee begint Nederland langzaam maar zeker naar een Politiestaat niveau af te glijden en daarom wordt het hoog tijd dat hier eens door de politiek een einde aan gemaakt wordt.

Hieronder een aantal maatregelen, maar dit is zeker geen complete lijst:

2001 Invoering van de AFTAP-verplichting voor internet verkeer.
2002 De politie mag preventief fouilleren.
2005 Algemene identificatieplicht.
2006 RFID in passpoort (draadloos op afstand uit te lezen)
2006 Alle openbare aanbieders van email en internet moeten NAW gegevens van klanten dagelijks doorgeven aan het CIOT.
2006 Camera toezicht zonder 'toezicht' neemt toe.
2007 AIVD heeft toegang tot alle IND gegevens.
2007 Anoniem reizen in het openbaar vervoer niet meer mogelijk door ov-chipkaart.
2008 Invoering breed toegankelijk elektronisch kind-dossier.

2009 Voorlopige afwijzing verplichte slimme energie-meters.
2009 Invoering electronisch patienten dossier.
2009 Bewaarplicht alle meta-informatie via de 'Europese route' tegen de wil van de 2e kamer.
2009 Locatie informatie GSM moet ook 6 maanden opgeslagen worden.
2009 Biometrische kenmerken in paspoort (protesten VN tegen vingerafdruk in paspoort)
2009 Uitbreiding DNA database.

Voor een overzicht verwijzen we naar de volgende links:
Column van *Karin Spaink*
Netkwesties met dit artikel in 2006
Beveiligingsite Security.nl met een aantal links.