Wilt u de totale informatie?
Essay: Prism en de informatieoorlog

Door: E.J. Dommering
Verschenen in: *De Groene Amsterdammer*, 26 juni 2013

De Prism-zaak laat onomwonden zien dat de Amerikaanse staat nauwelijks nog grenzen kent en op grove wijze de privé-sfeer van burgers betreedt. In Europa zou zoiets nooit mogelijk zijn – denken we. Of hopen we dat vooral?

IN DE REL ROND PRISM – het op grote schaal door de Amerikaanse overheid registreren van al het telefoon- en internetverkeer tussen burgers dat via Amerikaanse centrales of Amerikaanse servers verloopt– komen een aantal ontwikkelingen samen. De schaal waarop door de Amerikaanse Veiligheidsdienst wordt afgeluisterd en geregistreerd is nu kwantitatief zodanig dat er duidelijk een grens is overschreden. Er wordt geen maat meer gehouden, er is geen proportionaliteit meer.

De oorlog tussen soevereine staten wordt allengs vervangen door een oorlog van de staat tegen informatiedoelen (en dat zijn vaak individuen zonder staatsgezag) binnen of buiten het grondgebied van de staat. Zo past het op grote schaal registreren van individuele communicaties naadloos op het op grote afstand doden van individuen door middel van drones op grond van informatie over niet-statelijke doelen.

De rechtsstatelijke eisen die wij plachten te stellen aan het toepassen van overheidsmacht en overheidsgeweld tegen individuen zijn aan het vervagen. In de oorlog tegen informatiedoelen gaan de regels van oorlogvoering gelden in plaats van de regels van de rechtsstaat. Dat proces wordt versterkt doordat de uitoefening van staatsmacht en staatsgeweld niet meer aan het territoir is gebonden, zodat we niet meer weten welke nationale wettelijke regels er gelden en welke nationale rechters bevoegd zijn om in te grijpen. Daarmee raakt het individu dat

informatiedoel is verzeild in een rechtsvacuüm tussen de staat van oorlog en de staat van het recht.

De 'big data'-technologie die het op grote schaal vergaren van gegevens interessant maakt, heeft het begrip persoonsgegeven – dat het individu nog enig houvast gaf om de controle over zijn persoon te behouden – ineffectief gemaakt. Bovendien vergroot het het aantal overheids-interventies. We spraken voorheen over 'crime fighting', voortaan kunnen we het beter hebben over 'precrime fighting'.

De opeenhoping van informatie bij de overheid heeft de wetten van openbaarheid die op een proportionele manier probeerden transparantie van overheidsmacht te bereiken, ingehaald. Disproportionele verzamelzucht leidt tot disproportionele openbaarheid. De staat is een ommuurde informatiebureaucratie geworden, een informatiebunker die 'gewapenderhand' met digitaal tankgeschut genomen moet worden. De wetten van openbaarheid van bestuur maken plaats voor informatieterrorisme zoals WikiLeaks, waarvan Edward Snowden ook een manifestatie is. Ook in dit opzicht is het dus een informatieoorlog.

DE VERZAMELING VAN PERSOONSGEGEVENS door de staat kwam in de negentiende eeuw op gang en diende aanvankelijk het doel de burgers van de staat private en burgerrechten te verschaffen: een huis en een naam, staatsburgerschap en staatsburgerrechten. Maar ook veiligheid. Die veiligheid vormde echter een gescheiden circuit dat aan strenge regels van strafrecht en strafvordering was gebonden. De staat mocht pas in de privé-sfeer van burgers treden wanneer er een redelijk vermoeden van schuld aan een strafbaar feit bestond.

In de twintigste eeuw vormden de sociale welzijnsstaat en de steeds krachtiger consumenteneconomie de motoren om steeds meer en steeds verfijndere persoonsgegevens te verzamelen. Dit alles om de publieke of de private dienstverlening te bevorderen. Dit deed het verlangen ontstaan om proactief en preventief te werk te gaan: niet 'after the fact', maar 'before the fact'. De utopie was het veilige en gezonde welzijn van de mensheid. Controle van de privé-sfeer werd hoe langer hoe meer identiek aan veiligheid. De commissie-Brouwer-Korf die de Nederlandse regering in 2010 over veiligheid en privacy adviseerde smolt beide begrippen moeiteloos samen.

9/11 heeft het veiligheidsverlangen omgezet in een brede preventieve controle van de gedragingen van individuen. Het verband met gepleegde stafbare feiten werd verlaten. Dat noemt men 'crowd control'.

Op het niveau van terrorismebestrijding heeft de Prism-zaak verschillende voorlopers. Een daarvan is het Echelon-project. Ongeveer zestien jaar geleden begon de Nationale Amerikaanse Veiligheidsdienst (NSA) via het Verenigd Koninkrijk op grote schaal satellietverkeer af te tappen (een groot deel van het telefoon- en e-mailverkeer tussen Europa en de VS loopt via satellieten). Ergens in het noorden van Yorkshire ligt in een idyllisch landschap een complex met een verzameling enorme bollen die eruitzien als witte golfballen. Dit complex (dat Menwith Hill heet) draagt de misleidende aanduiding 'operatie van de Royal Air Force'. Dat is het niet. De Engelse luchtmacht verhuurt het terrein aan de NSA. In feite worden hier op aanwijzing van de NSA gegevens van afgevangen vertrouwelijk satellietverkeer opgeslagen.

Deze operatie berust op een overeenkomst tussen de VS en het Verenigd Koninkrijk en andere Engelstalige landen (de zogenaamde UKUSA-staten). De wettelijke basis in de VS is de Communications Assistance Law Enforcement Act (CALEA) die nog onder het presidentschap van Clinton in 1994 is aangenomen. Menwith Hill is dus geen gasopslag, wat je op het eerste gezicht zou denken. Het zijn de kristallen bollen waarin de Engelstalige veiligheidsdiensten kijken of individuen geen gevaarlijke dingen aan het plannen zijn. Wie weet ligt daar wel de planning van de aanslag op 9/11 onder het datastof verborgen, als een nooit gevonden schat die na duizend jaar door informatie-archeologen zal worden ontdekt.

De operatie bleef lange tijd geheimzinnig, en de Europese pers bleef terughoudend. Totdat er enige politieke beweging kwam toen het parlement van de Europese Unie in 2001 een rapport publiceerde (A5-264/2001) met een grondige analyse van de operatie. De juridische paragraaf van het rapport is onthullend: die stelt kort samengevat vast dat de juridische bescherming van EU-burgers ontoereikend is, omdat de CALEA niet de belangen en privacyrechten van EU-burgers beschermt en niet de strenge waarborgen bevat van artikel 8 van het Europees Verdrag voor de Rechten van de Mens.

Inmiddels is voor EU-burgers ook het grondrechtenhandvest van de EU van kracht geworden dat in artikel 8 nog eens een specifieke bepaling voor dataverkeer en -opslag bevat. De paragraaf in het rapport zou nu ook om andere redenen scherper geformuleerd moeten worden. Het Europees Hof voor de Rechten van de Mens deed in 2008 immers uitspraak over het preventief afvangen in het VK van al het communicatieverkeer tussen Ierland en Engeland met het systeem Electronic Test Facility (ETF) dat sinds de jaren negentig actief is. Die uitspraak kwam erop neer dat de categorie personen die mogen worden afgeluisterd nauwkeurig moet zijn afgebakend en dat er wettelijke waarborgen moeten zijn omtrent de duur en het gebruik van opgeslagen data en over de vernietiging ervan.

Dit rapport leidde tot enige discussie in Europese en nationale parlementen, maar daarna werd het weer stil. Ik weet niet of Echelon nog in dezelfde omvang functioneert (bijvoorbeeld als schakel in Prism; er zijn ook verdenkingen dat het voor drone-navigaties wordt gebruikt). In de publieke vergetelheid is het wel geraakt, omdat de meeste parlementariërs en commentatoren zich in het Prism-debat Echelon niet of nog maar met moeite konden herinneren.

In de VS is men na of naast Echelon vrolijk verder gegaan. In 2002 werd daar door de Defense Advanced Research Projects Agency (Darpa, uit wier schoot ooit het internet is geboren) de Information Awareness Office (IAO) opgericht met als doelstelling om de wereld van de Total Information Awareness (TIA) te bereiken. Als gevolg van 9/11 werd het TIA-programma omgesleuteld tot een programma om een contraterrorisme-informatie-infrastructuur te bouwen. Anders dan bij het Echelon-project ontbrak iedere wettelijke basis, wat een reden was voor de Senaat (en later het Congres) om de ontwikkeling van TIA in 2003 stil te leggen. TIA kreeg dan ook geen financiering meer. Na het stilleggen van het TIA-programma gingen de ontwikkelingen onder een andere naam verder. In 2007 bracht de NSA het project onder bij een al sinds 1970 actieve 'Special Source Operation' onder de naam Prism, waarin wordt samengewerkt met een honderdtal Amerikaanse 'trusted companies'.

De wettelijke basis voor deze activiteit was ook kwestieus, maar dat is onder George Bush in 2008 gladgestreken door de introductie van onder meer de Patriot Act ('Patriot' staat voor 'Providing Appropriate Tools for the Intercept and Obstruction of Terrorism') en een aanvulling van de Foreign Intelligence Surveillance Act (FISA). In die laatste wet is ook voorzien in de geheime rechtbank de Foreign Intelligence Surveillance Court (de FISC), die de Prism-activiteiten naar Amerikaanse maatstaven met niet op tegenspraak gegeven stempelbeslissingen heeft 'gelegaliseerd'. Dit zijn de zogenaamde FISC-orders die ook in het debat over Prism naar voren kwamen. En de NSA bouwt inmiddels in de woestijn in Utah een energie verslindende databunker van dimensies waarbij Menwith Hill in Yorkshire een verzameling pingpongballetjes lijkt. De piramides van de 21ste eeuw bestaan uit datagraven en de farao's van de geheime dienst willen steeds grotere hebben.

Ook uit het taalgebruik blijkt dat het om een militaire operatie gaat: er is diezelfde voorkeur voor afkortingen en codenamen. Inhoudelijk wordt de privacyvraag weggeschoven (door het Duitse Constitutionele Hof ooit omschreven als het recht om onbespied door het leven te gaan) – als we een terreuraanval weten te onderscheppen, dan rechtvaardigt dat alle privacy-inbreuken. Dat is het denken van de veldheer die met een kijker vanuit de militaire stelling de horizon afspeurt. Eén verdacht bewegend stipje, en BOEM! Niet geschoten is mis geschoten. Over effectiviteit en proportionaliteit van het bouwen van al die dataverzamelingen wordt niet gesproken.

DE PRISM-DISCUSSIE MAAKT PIJNLIJK DUIDELIJK dat het internet weliswaar de brenger van communicatievrijheid voor de hele wereld is, maar dat het een infrastructuur is die zich grotendeels in de rechtssfeer van de VS bevindt en waarover de VS vrijwel ongecontroleerde macht uitoefenen. Toch is er in de VS geen breed draagvlak voor de maatregelen. Uit een recente enquête van het weekblad Time bleek dat 63 procent van de ondervraagden bang is dat de verkregen informatie wordt misbruikt. De Amerikaanse belangenorganisatie die opkomt voor de handhaving van grondrechten, de ACLU, heeft op 13 juni een constitutionele actie tegen de NSA voor de New Yorkse rechtbank gebracht waarin ze Prism aanklaagt wegens schending van de Amerikaanse grondwet. Een dag eerder diende ze onder de Amerikaanse Wet openbaarheid van bestuur een vordering bij de rechter in waarin ze vroeg om openbaarmaking van de geheime FISC-orders. Daarvoor had ze al een verzoek ingediend bij het ministerie van Justitie om duidelijkheid te verschaffen over de geheime toepassing van de Patriot Act.

Moet Europa stilzwijgend toezien, omdat het zich allemaal afspeelt in de Amerikaanse rechtssfeer? Er zijn verschillende redenen waarom mij dit onjuist lijkt.

De acties bij de Amerikaanse rechters gaan over de belangen van Amerikaanse staatsburgers, niet over de wereldwijde gebruikers van internet. Het speelt zich dus niet uitsluitend af in de Amerikaanse rechtssfeer. Het optreden van de Amerikaanse overheid is in flagrante strijd met de opvattingen over privacybescherming in Europa: de wettelijke criteria voor toepassing zijn ontoegankelijk en duister, de procedurele waarborgen zijn onvoldoende omdat de rechterlijke controle geheim is, en het middel wordt disproportioneel ingezet. Onder de gevolgen van dat onrechtmatig handelen lijden de gebruikers in Europa: onze gesprekken, e-mails en internetpaden worden immers geregistreerd en bewaard. Dat is naar algemene opvatting een omstandigheid die bevoegdheid kan scheppen voor de rechter van het land van het slachtoffer. Het is onaanvaardbaar dat door het enkele feit dat een groot deel van de communicatie over in de VS gelegen telecommunicatie-infrastructuur van internet loopt het privacybeschermingsniveau dat wij in Europa hebben opgebouwd wordt verlaagd naar wat een geheime rechtbank in de VS op basis van een obscure Amerikaanse wetsbepaling denkt dat goed is voor de veiligheid van Amerika.

Bovendien schept artikel 8 van het Europese Verdrag voor de Rechten van de Mens een positieve verplichting voor de regering van de verdragsstaten om actief maatregelen te nemen om de privacy van de burgers te beschermen. Nederland is niet zo lang geleden gevoelig door het Europees Hof op de vingers getikt omdat het te weinig had gedaan om identiteitsfraude op zijn grondgebied actief te bestrijden. De EU en Nederland moeten dus diplomatieke actie

ondernemen tegen de Amerikaanse afluisterpraktijken. Die urgentie leeft niet bij de politiek, gezien de tamelijk lauwe reacties op het Snowden-lek, zowel nationaal als Europees. De kort geleden door de regering naar buiten gebrachte Mensenrechtennota zegt wel dat Nederland het instrumentarium van de EU actief wil inzetten om op te komen tegen ernstige mensenrechten-schendingen, maar zwijgt geheel over het probleem van de ernstige privacyschendingen op internet.

President Obama heeft zich ter verdediging van het optreden van de NSA erop beroepen dat er slechts 'metadata' worden geregistreerd: waar en wanneer is er met wie gebeld of gemaild. Afgezien van het feit dat The Guardian stelt over gelekte FISC-orders te beschikken waaruit blijkt dat de observaties veel verder gaan en dat het rechterlijk toezicht niets voorstelt (door de krant getypeerd als een 'vijgenblad') is er iets anders aan de hand. We stuiten hier op de door mij gesignaleerde laatste trend van de ontwikkeling naar big data. Wij weten uit de geschiedenis van het data verzamelen dat ogenschijnlijk neutrale gegevens toch veel over personen kunnen zeggen. Postcodes zeggen iets over het welzijnsniveau van de woonwijk waaraan ze zijn toegekend. Als zodanig verschaffen zij direct-marketingbedrijven waardevolle tot personen herleidbare informatie.

TOEN WIJ EEN AANTAL JAREN GELEDEN in Europa de discussie hadden over de dataretentierichtlijn die de plicht schept voor telefoon- en internetbedrijven om het soort gegevens dat nu in de VS wordt opgeslagen gedurende zekere tijd te bewaren, was het geen vraag of dit tot personen herleidbare gegevens zijn. Waar, wanneer en met wie je hebt gebeld of gemaild is dikwijls waardevollere informatie dan wat er wordt gezegd en geschreven. Het verschil met de VS is echter dat de gegevens hier door de betrokken ondernemingen moeten worden bewaard, maar dat in de VS de NSA er direct toegang toe krijgt om ze te analyseren. En de mogelijkheden van statistische analyses die uit ogenschijnlijk neutrale gegevens informatie over individuele gedragingen blootleggen, nemen met de dag toe.

Zoals internetspecialist Viktor Mayer-Schoenberger het in het jongste nummer van Foreign Affairs simpel onder woorden brengt: 'Het idee van "big data" is dat we uit een grote verzameling informatie dingen kunnen leren die wij niet hadden kunnen begrijpen als we een kleine hoeveelheid zouden hebben gebruikt.' Het gaat er dus om dat de NSA met die geheime FISC-orders zo veel mogelijk data in handen krijgt. En dat is dus het tegenovergestelde van het proportionaliteitsbeginsel dat wij bij noodzakelijke privacybeperkingen plachten te hanteren.

Maar big data betekent ook een omwenteling van hoe wij naar de werkelijkheid kijken. Het is wat de Amerikaanse wetenschapper Philip Agre al in 1997 de 'spiegelwereld' noemde: de wereld van de data en de computerschermen vervangt de echte werkelijkheid. Uit de maalstroom van data

verschijnen na krachtige bewerkingen op computerschermen patronen en connecties. Die zijn het informatiedoel. Obama heeft met de big data-analysetechniek een inert deel van het Amerikaanse electoraat naar de stembus weten te krijgen en er de verkiezingen mee gewonnen. Hij hoopt er nu 'the war on terror' mee te winnen. En wat meer is: hij hoopt deze op den duur te herleiden tot datastructuren op een computerscherm: een onzichtbare spiegel van de werkelijkheid, waar hij politiek geen last van heeft.