Betreft: Reactie Consultatie Wet op de inlichtingen- en veiligheidsdiensten 20..

New York & Amsterdam, 29 augustus 2015

Het door de Nederlandse regering ter consultatie openbaar gemaakte voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten roept een aantal fundamentele vragen op. In het bijzonder is er naar ons oordeel en onze deskundigheid sprake van de volgende gebreken:

1. Onvoldoende waarborgen bij verzameling en analyse van (persoons)gegevens;
2. Hacking en doorzoeking van binnenlandse communicatie zijn onvoldoende beteugeld;
3. Gebrek aan transparantie ondermijnt de legitimiteit van de diensten;
4. Geen effectieve waarborgen rondom de bevoegdheid tot data-mining;
5. Te weinig harde grenzen aan toegang tot data en bestanden;
6. Te smalle blik op het grondrechtelijk kader;
7. Slechte regeling rondom bijzondere en gevoelige gegevens;
8. Onvoldoende handvatten voor de subsidiariteitstoets.

Het is ons oordeel dat deze gebreken, die wij in het navolgende toelichten, op het punt van de inbreuk op de mensenrechten en andere democratische belangen van zo'n ernstige aard zijn dat zij aanleiding vormen het voorstel te herzien.

Het recht dient om de macht te beteugelen. Juridische en technologische structuren waarin uiteindelijk slechts de onder maatschappelijke tijdgeest veranderlijke definitie van "nationale veiligheid" de grens vormt aan inzet van bevoegdheden, schieten wat dat betreft tekort.

dr. J.V.J. van Hoboken, Postdoctoral Research Fellow, New York University, School of Law; Gastonderzoeker, Universiteit van Amsterdam, Instituut voor Informatierecht (IviR) (op persoonlijke titel);

en

dr. M.R. Koot, IT-beveiligingsconsultant bij Madison Gurkha; extern deelnemer bij het Amsterdam Platform for Privacy Research, Universiteit van Amsterdam (op persoonlijke titel).

**** In herinnering aan Caspar Bowden ****

1. Onvoldoende waarborgen bij verzameling en analyse van (persoons)gegevens

Het wetsvoorstel gaat uit van een stelselmatige vergroting van de algemene mogelijkheden tot het verkrijgen van (persoons)gegevens uit de samenleving (Artikel 22) alsmede het gebruik daarvan, waaronder voor data-analyse (Artikel 47). In het bijzonder is sprake van de mogelijkheid tot het verkrijgen van **directe toegang** tot gegevensbestanden, alsmede het verkrijgen van toegang tot **gehele bestanden** door overdracht aan de diensten.

De **kring van personen waarover gegevens** mogen worden verwerkt door de diensten is tevens **uitgebreid** met het kennelijke doel om maximale collectie gebruik van gegevens een juridische basis te geven. Specifiek wordt het mogelijk om gegevens te verkrijgen en verwerken van personen "indien die gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden" (Artikel 18, vijfde lid). Deze eis lijkt erg zwak geformuleerd.

De voorgestelde uitbreiding van bevoegdheden komt niet uit de lucht vallen, maar bij de geschiedenis wordt selectief stilgestaan. De zogenaamde **post-Madrid voorstellen** bevatten reeds de nieuwe bevoegdheden voor het verkrijgen van gehele bestanden, alsmede directe toegang daartoe. Opmerkelijk is echter dat de toen voorgestelde waarborgen in het huidige voorstel grotendeels ontbreken.

In het bijzonder zijn de voorgestelde bevoegdheden tot het verkrijgen van gegevens(bestanden) en directe toegang daartoe, alsmede de toepassing van data-mining daarop, in het voorstel **geregeld als gewone bevoegdheden**, in tegenstelling tot de vergelijkbare post-Madrid voorstellen. De extra waarborgen voor bijzondere bevoegdheden (bevoegdheden die vanuit hun inbreukmakende aard een specifiekere regeling behoeven, en meer waarborgen vereisen) zijn daarmee niet van toepassing. Het is **niet verdedigbaar** om deze bevoegdheden niet te te kwalificeren als bijzondere bevoegdheden met de nodige extra waarborgen. De Memorie van Toelichting (MvT) bij het concept laat na om de stelselmatige inbreuk die de voorgestelde artikelen 22 en 47 mogelijk maken op de grondrechten van Nederlandse burgers, organisaties en andere betrokkenen te verantwoorden.

Voor het verkrijgen van een handvol gegevens van een bedrijfje dat over wat gegevens beschikt (over een specifiek persoon die onderwerp is van onderzoek door een dienst), geldt dezelfde regeling (met dezelfde minimale waarborgen) als de stelselmatige toegang tot gegevens van bijvoorbeeld de Belastingdienst, alle gegevens van het gebruik van de OV-chipkaart, of de beheerder van de digitale paspoortgegevens van Nederlandse burgers. Dit is **zowel vanuit grondrechtelijk en maatschappelijk perspectief als vanuit wetstechnisch perspectief onacceptabel**. Ter vergelijking, in de huidige wettelijke regeling die de overheid toegang tot gegevens biedt in het kader van strafvordering (Wet bevoegdheden vorderen gegevens van 2006) is een trapsgewijs systeem van grondslagen en scherpere waarborgen geregeld voor het verkrijgen van gegevens, al naar gelang de verkrijging een zwaardere inbreuk maakt op de belangen en persoonlijke levenssfeer van betrokkenen.

Het **vrijwillige karakter van de verstrekking** op basis van Artikel 22 kan niet als verzachtende

omstandigheid worden aangevoerd in dit verband. Immers, de vrijwilligheid maakt de bevoegdheid **niet minder ingrijpend** voor de personen waarop de gegevens betrekking hebben. Daarbij komt dat deze vrijwilligheid zelf een aantal vragen oproept. Waarom is gekozen voor vrijwilligheid? Is het acceptabel en mogelijk dat organisaties een eigen afweging maken over de vraag of gegevens verstrekt zouden moeten worden bij een verzoek? En als dat al het geval is, op basis van welke gegevens zouden deze organisaties een afweging moeten kunnen maken over de vraag of inderdaad verstrekt dient te worden? Het is opmerkelijk dat 10 jaar na de keuze voor het verlaten van de systematiek van vrijwilligheid van verstrekking van gegevens aan de overheid (mede in navolging van Rapport Commissie Mevis) nu weer is gekozen voor deze vrijwilligheid in het voorgestelde wettelijk kader. In de voorbereiding op het uiteindelijke wetsvoorstel is te weinig aandacht geweest voor deze vraag en er dient toelichting te worden gegeven op de vraag in hoeverre vrijwilligheid in de praktijk een drempel heeft gevormd of toch te verkiezen is boven een regeling van verplichte verstrekking.

Bij de beoordeling van deze voorstellen voor artikelen 22 en 47 dient door de wetgever te worden erkend dat in de huidige samenleving over **alle aspecten van het leven van personen** (sociaal, economisch, medisch, politiek, cultureel, religieus) **grote hoeveelheden gegevens** worden verzameld en gebruikt door publieke en private instanties. In veel gevallen geven deze bestanden een veelomvattend en zeer indringend beeld van de betreffende aspecten van het leven van personen. In samenhang bezien (immers, de diensten kunnen de gegevens vervolgens ook koppelen) ontstaat een zeer veelomvattend beeld van personen. Dit beeld kan puur op basis van de inzet van artikelen 22 en 47 details bevatten waarover de diensten in het papieren tijdperk maar in grote uitzondering beschikking over hadden kunnen krijgen, door de structurele inzet van traditioneel als ingrijpend geachte bevoegdheden zoals afluisteren, infiltratie en observatie. De explosieve groei van de beschikbaarheid van gegevens in de samenleving is daarmee op zichzelf al een reden om de bestaande mogelijkheid van toegang tot deze gegevens door de diensten kritisch te bekijken en herzien.

Daar komt ten slotte bij dat het zonder strikte waarborgen exploiteerbaar maken van gegevens elders door de diensten de relatie van burgers tot de organisaties die deze gegevens verzamelen en gebruiken kan schaden. De **sociale, maatschappelijke en economische schade** die een dergelijke **vertrouwensbreuk** en bijkomende onwil om gegevens af te staan voor legitieme doelen veroorzaakt wordt door het wetsvoorstel niet onderkent, noch besproken.

Het is gezien het bovenstaande noodzakelijk om de voorgestelde regeling in artikelen 22 en 47 te herzien, waarbij de volgende uitgangspunten meegenomen kunnen worden:

- **Een getrapte regeling:** voor de verkrijging van gegevens zou een getrapte regeling moeten gelden met specifiekere eisen aan uitvoering en zwaardere waarborgen voor verwervingen die als ingrijpender en meer inbreukmakend moeten worden gekwalificeerd;
- **Bijzondere bevoegdheden:** bij het verkrijgen van gevoelige gegevens, gehele bestanden of directe toegang dient de bevoegdheid tot het verkrijgen van gegevens te worden opgenomen in het hoofdstuk bijzondere bevoegdheden;
- **Bijzondere bronnen:** er dienen veel striktere waarborgen of verboden te gelden voor het verkrijgen van gegevens van maatschappelijke organisaties die naar hun aard een bijzondere maatschappelijke taak vervullen die zich slecht verhoudt tot de stelselmatige verstrekking van

gegevens aan inlichtingen en veiligheidsdiensten (scholen, universiteiten, bibliotheken, media, politieke organisaties en bewegingen, et cetera.). Bij dergelijke organisaties is het verkrijgen van directe toegang of gehele bestanden naar zijn aard een onaanvaardbare maatschappelijke inbreuk.

- **Gehele bestanden alleen bij uitzondering:** de toets voor het verwerken van gehele bestanden (omdat de gegevens "onlosmakelijk verbonden" zijn met gegevens waarvoor een grondslag is) moet veel scherper worden gesteld.
- **Scherp toezicht op risico's data-mining:** De mogelijkheid van toezicht op de risico's van data-analyse moet beter worden geregeld in Artikel 47. In het bijzonder dient wettelijk de mogelijkheid van toezicht op de gebruikte algoritmes en de behandeling van foutpositieven en foutnegatieven worden vastgelegd alsmede toezicht op de vraag of bepaalde personen en groepen een onevenredig risico lopen door data-analyse onterecht als risico of doel van verder onderzoek te worden aangemerkt.
- **Advies van het CBP over het wetsvoorstel:** gezien de gevolgen voor het vertrouwen in de bescherming van persoonsgegevens in de rest van het maatschappelijke domein ligt het in de rede advies aan het CBP te vragen over de voorgestelde regeling in artikelen 22 en 47.

2. Hacking en doorzoeking van binnenlandse communicatie: beteugel de macht

Het kabinet wil de diensten toestaan om "**alle vormen van communicatie**" van (ook) onverdachten in bulk te doorzoeken op identiteiten, technische kenmerken en trefwoorden, en te koppelen aan andere gegevens. Op de uitoefening van die bevoegdheden zijn weliswaar de eisen van doelgerichtheid, noodzakelijkheid, proportionaliteit en subsidiariteit van toepassing, maar die eisen worden door het kabinet niet onverenigbaar geacht met bulkverwerkingen: immers codificeert het wetsvoorstel nu juist (grootschalige) verwerkingen van metadata (Artikel 35), verruimt het de bulkinterceptiebevoegdheid (Artikel 33), en komt het ook bij gegevens verworven via de hackbevoegdheid (Artikel 30) en de regeling van vrijwillige gegevensverstrekkingen (Artikel 22) neer op de **in potentie grootschalige verwerking van gegevens van (ook) non-targets**.

De definitie van communicatiedienst is blijkens de MvT zo ruim dat eigenlijk alle informatiesystemen (inclusief opslag en bestanden) die transmissie van gegevens mogelijk maken onder de reikwijdte van dit begrip lijkt te komen te vallen. Dit heeft het onwenselijke gevolg dat er voor al deze ICT dezelfde voorwaarden gelden voor inbreukmakend handelen door de diensten, middels bijzondere bevoegdheden zoals binnendringen van systemen. Dit is niet in overeenstemming met het vereiste van voorzienbaarheid en proportionaliteit. Het ligt in de reden om scherpe voorwaarden te stellen voor specifieke ICT, zoals telecommunicatie (privé), cloudopslag (onderscheid naar klant nodig), hosting van content voor publieke toegang, et cetera. De ruime definitie zorgt ook voor een zeer grote overlap van Artikel 22 met Artikel 30.

De definitie kan bovendien bij Algemene Maatregel van Bestuur worden bepaald, en dat ondermijnt de voorzienbaarheid: de minister krijgt speelruimte, terwijl burgers en organisaties in onzekerheid zitten over de impact die de wet op hen heeft. Over de medewerkingsplichten die op de aanbieders rusten (toegang tot netwerken ex Artikel 37, de verstrekking van verkeersgegevens ex Artikel 39 en de verstrekking van abonneegegevens ex Artikel 40) kan worden opgemerkt dat deze de facto een

herintroductie vormen van een controversieel onderdeel van het post-Madrid voorstel van gedwongen, grootschalige gegevensverstrekkingen door derden - in dit geval communicatiediensten. **Duidelijkheid over de reikwijdte van het begrip "aanbieder van een communicatiedienst" is dus van cruciaal belang om het wetsvoorstel te kunnen beoordelen op noodzaak en proportionaliteit.**

De voorzienbaarheid wordt eveneens ondermijnd door het **ontbreken van duidelijkheid over de relatie tussen de hackbevoegdheid ex Artikel 30 en de bulkinterceptiebevoegdheid ex Artikel 33.** Namelijk:

- **Mag toegang die op grond van de medewerkingsplicht ex Artikel 37 wordt verkregen tot een communicatienetwerk door de diensten worden gebruikt om de hackbevoegdheid ex Artikel 30 uit te oefenen?** Dat is plausibel in het kader van "man in the middle"-aanvallen tegen smartphones, computers en netwerken, door netwerkverkeer te injecteren en/of manipuleren. Uit de Snowden-documenten is duidelijk geworden dat deze tactiek bij Britse en Amerikaanse diensten staande praktijk is. Zulke aanvallen kunnen bij uitstek worden uitgevoerd via de systemen en netwerken van aanbieders van communicatiediensten. Passief luisteren en actief manipuleren hebben een verschillende impact op het netwerk van de aanbieders en de communicatie van hun klanten. Duidelijkheid over de vraag of de in het kader van bulkinterceptie afgedwongen toegang óók mag worden ingezet ter ondersteuning van de uitoefening van de hackbevoegdheid is daarom van belang.

- **Mag de hackbevoegdheid ex Artikel 30 worden ingezet ter ondersteuning van het in bulk verwerven dan wel doorzoeken of selecteren van communicatie ex Artikel 33 t/m 35?** Artikel 30 mag volgens de bepaling in het tweede lid, onder c, worden gebruikt ter ondersteuning van gerichte interceptie ex Artikel 32, maar er is geen verwijzing naar Artikel 33, 34 of 35. Mag daaruit worden geconcludeerd dat het de diensten niet is toegestaan de hackbevoegdheid uit te oefenen ter ondersteuning van deze bevoegdheden? Het maakt immers verschil of de hackbevoegdheid wordt ingezet tegen de smartphone van één target om gericht af te luisteren, of tegen de systemen van een telecomprovider om daar de bulk van communicatie te doorzoeken waar de diensten anders geen toegang tot hebben: dat laatste raakt in potentie de rechten van grote groepen personen. Indien het de bedoeling is de hackbevoegdheid voor hiertoe in te zetten, dan is het van belang dat er helderheid komt over de vraag onder welke voorwaarden die inzet wel en niet voldoet aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.

Zoals hoogleraar informatiebeveiliging Bart Preneel (KU Leuven) stelt: alomtegenwoordige surveillance vraagt om alomtegenwoordige gegevensverzameling en digitale aanvallen die nevenschade veroorzaken aan ICT-infrastructuur.[1] Bij aanvallen gericht op buitenlandse ICT-infrastructuur moet bovendien worden gewaakt voor digitaal kolonialisme. **Het is de vraag hoe noodzaak, proportionaliteit en subsidiariteit in voorkomende toepassingen van de hack- en bulkinterceptiebevoegdheden moeten worden beoordeeld.**

1 Bart Preneel, 2 juni 2015: "System Security after Snowden". Slides. Link (.pdf): http://homes.esat.kuleuven.be/~preneel/preneel_snowden_dsn15_v1.pdf

Voorts is er de vraag van de noodzaak van de nieuwe bulkinterceptiebevoegdheid: **voor welke doelstellingen is bulkinterceptie van binnenlandse en buitenlandse communicatie wérkelijk noodzakelijk, en waaruit blijkt dat**? Voor terrorismebestrijding zijn de noodzaak en subsidiariteit van bulkinterceptie bijvoorbeeld geenszins aangetoond. Vanuit de Verenigde Staten lijken er eerder aanwijzingen van het tegendeel. Zo stelt de New America Foundation in januari 2014 na onderzoek dat de massale verwerking van metadata van binnenlandse telefoongesprekken "no discernible impact" heeft gehad op het voorkomen van terroristische handelingen, en "only the most marginal of impacts" op het voorkomen van terrorismegerelateerde activiteiten, zoals fundraising.[2] Dat beeld is in mei 2015 nog eens bevestigd door de inspecteur-generaal van de FBI.[3]

Plotselinge gewelddadige acties van eenlingen worden via bulkinterceptie waarschijnlijk niet voorkomen. Bovendien bestaan in Nederland al ruime bevoegdheden op het vlak van terrorismebestrijding, en is niet duidelijk waarom deze, in samenhang met tal van activiteiten die worden ondernomen niet reeds voldoende zouden zijn voor het bestrijden van terroristische dreigingen.

De wettelijke taken waarvoor de diensten bijzondere bevoegdheden mogen toepassen, zijn in abstracte termen limitatief beschreven in de wettelijke taakstellingen. Maar **de volgens die taken te beschermen belangen zijn soms zeer ruim**. Dat geldt in het bijzonder voor de veiligheidstaak van de AIVD ("a-taak"), betreffende "het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat". Onder "veiligheid van de staat" valt "nationale veiligheid", en dat begrip laat zich slecht afbakenen. **Het toestaan van bulkverwerking in het kader van de nationale veiligheid vormt een reëel risico voor de bescherming van de democratie en de rechten van personen die in of via Nederland communiceren**. Ter illustratie kan het "OPTIC NERVE"-programma worden genoemd, waarin het Britse GCHQ webcambeelden van miljoenen Yahoo-chatgebruikers wereldwijd van glasvezelkabels onderschepte met de bedoeling deze te doorzoeken op beeldpatronen.[4] Drie tot elf procent hiervan --- dus mogelijk honderdduizenden privéchats --- bevatten seksueel expliciete beelden. Dit is een grote inbreuk op de privacy van de betrokkenen, in het bijzonder als deze niet eens een onderwerp van gericht onderzoek zijn. Moeten burgers hun gedrag dan maar aanpassen, omdat er een reële kans is dat hun privébeelden als bijvangst worden gearchiveerd en doorzocht door de algoritmen van diensten? **We benadrukken in dit verband dat inbreuk op de persoonlijke levenssfeer al wordt gemaakt op het moment dat de gegevens door de diensten worden verzameld en met algoritmen worden onderzocht en doorzocht, en dus niet pas op het moment dat er uit de bulk wordt geselecteerd.**

Als tweede illustratie kan de Nederlandse docent wis-, schei- en natuurkunde in herinnering worden geroepen. Hij woonde ooit in dezelfde straat als atoomspion Kahn, zocht jaren later in het kader van het voorbereiden van Cito-examenvragen op internet naar "zwaar water", en werd daarover vervolgens met vragen benaderd door de AIVD.[5] De docent vocht daarna een vruchteloze strijd om

2 New America Foundation, 13 januari 2014: "Do NSA's Bulk Surveillance Programs Stop Terrorists?". Link: https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/

3 Washington Times, 21 mei 2015: "FBI admits no major cases cracked with Patriot Act snooping powers". Link: http://www.washingtontimes.com/news/2015/may/21/fbi-admits-patriot-act-snooping-powers-didnt-crack/?page=1

4 Wikipedia, "Optic Nerve (GCHQ)". Link: https://en.wikipedia.org/wiki/Optic_Nerve_%28GCHQ%29

5 NRC Handelsblad, 8 juli 2006: "'Of ze konden komen praten over massavernietigingswapens'". Link:

inzicht te krijgen in de informatie die over hem is verwerkt en de bevoegdheden die tegen hem zijn ingezet. **Kunnen non-targets straks maar beter niet over bepaalde onderwerpen communiceren of naar bepaalde informatie zoeken, willen ze voorkomen dat er naslag wordt gedaan in hun privéleven en de AIVD vragen komt stellen?** Kunnen jongeren bij maatschappijleer maar beter geen project kiezen waarin ze op internet moeten zoeken naar jihadistische propaganda? Hoe zit dat voor journalisten, advocaten, politici en de nieuwsgierige burger die zich graag via internet informeert over allerlei onderwerpen?

Inlichtingendiensten die uit praktische overwegingen zonder onderscheid tussen targets en non-targets geautomatiseerd privécommunicatie doorzoeken van grote groepen burgers inclusief journalisten, advocaten en politici: dat is geen acceptabele situatie voor een Nederlandse rechtsstaat. Indien gerichte bulkinterceptie aantoonbaar noodzakelijk is voor, bijvoorbeeld, het beschermen van militairen in het buitenland, zou het voor die specifieke doelstellingen kunnen worden toegestaan, en worden beperkt. **Het valt te betwijfelen of het enkele feit dat IP-verkeer automatisch een route via internet zoekt tot de conclusie moet leiden dat een buitenlandeis in geen enkele vorm mogelijk is, en dat in de wet in het geheel geen onderscheid kan worden gemaakt tussen binnenlandse communicatie en communicatie met een oorsprong of bestemming in het buitenland.** In het bijzonder dient die vraag te worden gesteld bij de searchbevoegdheid, die thans nog met een buitenlandeis is ingeperkt (Artikel 26 Wiv2002). Die bevoegdheid wordt immers ook ingezet voor verkennend onderzoek, waarbij geen aparte toestemming voor selectie nodig is. Van de MIVD is bekend dat communicatie vervolgens ook wordt geselecteerd op basis van "generieke identiteiten", die volgens de CTIVD soms "veelomvattend" zijn en die een ruime fuik vormen voor categorieën van personen.[6] Het idee dat op die manier zou kunnen worden gezocht en geselecteerd uit de bulk van ook *binnenlandse* communicatie is reden tot zorg. Een buitenlandeis vormt in elk geval geen belemmering voor onderzoeken die in het kader van militaire missies, non-proliferatie en de inlichtingentaak buitenland worden uitgevoerd.

We onderschrijven verder het belang van het bestaan van mogelijkheden om anoniem en vertrouwelijk te kunnen communiceren op internet, zoals dat in mei 2015 is uiteengezet door de speciale VN-rapporteur voor vrijheid van meningsuiting.[7] Voor binnenlandse en buitenlandse dissidenten en klokkenluiders, maar ook voor anderen die zich (terecht) zorgen maken over het vastleggen van online gedrag vanwege de mogelijkheid dat de vastgelegde gegevens in de toekomst tegen hun wensen en belangen opduiken in andere contexten. Gaan de diensten het versleutelde verkeer van het anonimiteitsnetwerk Tor in bulk onderscheppen en delen met buitenlandse diensten, om zo gezamenlijk Tor-gebruikers te deanonimiseren? Die vraagt vloeit voort uit de via Snowden onthulde notulen van een overleg tussen de AIVD en de NSA, waarin de NSA refereert aan een "multi-national effort" om Tor-verkeer te deanonimiseren.[8] De bewaartermijn voor bulkintercepts is niet van

http://vorige.nrc.nl/krant/article1700579.ece

6 CTIVD, "Toezichtsrapport 28 over de inzet van Sigint door de MIVD", 23 december 2011. Link: http://www.ctivd.nl/onderzoeken/t/toezichtsrapport-28/documenten/rapporten/2011/12/23/index

7 David Kaye, speciale VN-rapporteur op het gebied van vrijheid van meningsuiting, 22 mei 2015: "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". Te downloaden via: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

8 NRC Handelsblad, 30 november 2013: "AIVD hackt internetfora, 'tegen wet in'". Link: http://www.nrc.nl/nieuws/2013/11/30/aivd-hackt-internetfora-tegen-wet-in/

toepassing op versleutelde gegevens; versleuteld Tor-verkeer mag dus onbeperkt worden bewaard. Een mogelijke consequentie daarvan is dat de communicatie van Tor-gebruikers ook in de verre toekomst nog wordt gedeanonimiseerd. Zulke activiteit ondermijnt het vertrouwen in het Tor-netwerk, dat nu bij uitstek een relatief volwassen kanaal biedt om in enige anonimiteit op internet te kunnen handelen. In dit kader kan nog worden herinnerd aan het feit dat het de diensten is toegestaan om gegevens die in het kader van een bepaald onderzoek zijn verzameld, ook voor andere onderzoeken te gebruiken; en dat de diensten ex Artikel 83 "technische en andere vormen van ondersteuning" kunnen bieden aan met de opsporing van strafbare feiten belaste instanties, die ook interesse kunnen hebben in de deanonimisatie van Tor-verkeer.

In 1971 schreef het hoofd van de toenmalige Buitenlandse Inlichtingendienst in reactie op het voorstel om mensenrechtenverdragen expliciet van toepassing te verklaren op de diensten het volgende:

> *In deze tijd waarin men de zaken bij hun naam wil noemen moet erkend worden, dat koude oorlog óók oorlog is en dat het inlichtingenwerk nu juist NIET bij uitstek uit is op eerbiediging van menselijke rechten en waardigheden*.

Die stelling heeft helaas ook vandaag nog relevantie, getuige de onthullingen van Snowden, WikiLeaks en anderen. Uit CTIVD-toezichtsrapporten blijkt dat er al **jarenlang onzorgvuldigheden en onrechtmatigheden** voorkomen in de inzet van de selectiebevoegdheid ex Artikel 27 Wiv2002, betreffende bulkintercepts van ethercommunicatie. Ook bij de inzet van de search- en hackbevoegdheden ex Artikel 26 en Artikel 24 Wiv2002 heeft de CTIVD onzorgvuldigheden en onrechtmatigheden vastgesteld. In plaats van het uitbreiden van bevoegdheden zou het wetsvoorstel een betere garantie moeten bieden op rechtmatigheid van het handelen van de diensten onder de bestaande bevoegdheden.

3. Transparantie als voorwaarde voor legitimiteit van de diensten

Het kabinet ziet tot op zeker hoogte in dat uitbreiding van bevoegdheden vraagt om uitbreiding van waarborgen. Een essentiële waarborg die in het wetsvoorstel echter ontbreekt is het vastleggen en publiceren van statistieken die inzicht geven in het gebruik van die bevoegdheden. Dat inzicht is nodig voor zowel het interne toezicht als het toezicht door de Tweede Kamer en de CTIVD. Transparantie richting de samenleving als geheel alsmede in internationaal verband is ook een voorwaarde voor de democratische legitimiteit van de diensten en de internationale positie van Nederland als rechtsstaat.[9]

In België is in de wet verankerd dat de toezichthouder, het Vast Comité I, het parlement periodiek inzicht geeft in het aantal gegeven machtigingen voor de inzet van bijzondere bevoegdheden.[10] Dat gebeurt alleen voorzover dat de goede werking van de diensten niet aantast en de samenwerking tussen de Belgische en buitenlandse diensten niet in gevaar brengt. Uit de openbare

9 Naast de groeiende internationale trend van "transparency reporting" wordt het belang van deze transparantie over de inzet van ingrijpende bevoegdheden ook onderschreven in het IViR-rapport "Ten standards for oversight and transparency of national intelligence services" van juli 2015. Link (.pdf): http://www.ivir.nl/publicaties/download/1591

10 Artikel 35 van de Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Link: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1991071853&table_name=wet

toezichtsrapporten van het Vast Comité I wordt duidelijk dat deze voorwaarden nooit een belemmering hebben gevormd voor het publiceren van gedetailleerde cijfers. Naast Belgische burgers hebben ook de Duitse en Britse burgers inzicht in de omvang van de activiteiten van hun inlichtingendiensten, en ook in de Poolse wet is recentelijk een vereiste van publicatie van statistieken opgenomen. In Nederland werd de toezichthouder, CTIVD, door de minister gecensureerd toen zij enkele cijfers openbaar wilde maken. De toezichthouder laat daar in haar jaarverslag 2014-2015 geen misverstand over bestaan:

> "(...) De Commissie was en is het hier niet mee eens. De aantallen geven een indruk van de omvang van de inzet van deze bijzondere bevoegdheden, terwijl de buitenwereld hieruit niet kan afleiden tegen welke (categorieën van) personen en organisaties de inzet zich concreet richt. Het publiceren van aantallen is bovendien iets wat in ons omringende landen jaarlijks gebeurt".

Feit is dat er andere landen al jarenlang openbaar cijfers publiceren over de inzet van ingrijpende bevoegdheden en zich dus realiseren dat de vaak speculatieve nadelige gevolgen voor de taakuitoefening van diensten niet opwegen tegen het positieve effect van deze vorm van transparantie. Daarin is bovendien een aanwijzing te vinden dat op dit punt waarschijnlijk geen onbegrensde "margin of appreciation" bestaat in de uitleg van het begrip "nationale veiligheid". Een onbeargumenteerd beroep op deze "margin of appreciation" kan dus niet slagen als argument om geen cijfers te publiceren. Wij zijn van mening dat Nederland voorop dient te lopen met transparantie, en roepen de wetgever op de toezichthouder bij wet te verplichten statistieken te rapporteren over de inzet van ingrijpende bevoegdheden. Er kan, zoals in België, een beperkingsclausule worden opgenomen om openbaarmaking te voorkomen wanneer dat de effectiviteit van de diensten of hun samenwerkingsverbanden dreigt te schaden.

4. De bevoegdheid tot data-mining bevat geen effectieve waarborgen

Artikel 47 geeft een zeer ruime mogelijkheid tot data-analyse. Het bevat eigenlijk geen beperkingen. Artikel 47, tweede lid, maakt duidelijk dat het gaat om een niet limitatieve opsomming "immers de toepassing van eventuele nieuwe methoden en technieken moet mogelijk zijn" (MvT). De beperking in Artikel 47, derde lid, is geen echte beperking in de praktijk. Er is altijd sprake van aanvullende gegevens of menselijke tussenkomst bij het treffen van maatregelen. Dat is ook de ervaring met Artikel 15 van de Europese richtlijn 95/46/EC, dat een beperking oplevert voor automatiseerde beslissingen die uitsluitend gebaseerd zijn op geautomatiseerde verwerking van gegevens. De menselijke tussenkomst is terecht, maar het wordt steeds moeilijker vast te stellen of bepaalde personen of groepen terecht als risico worden aangemerkt, gezien de sterk gegroeide complexiteit van analysetechnieken. Zijn deze uitkomsten van data-analyse uiteindelijk nog wel goed te evalueren? Als alternatief voor deze simpel te omzeilen eis dat niet uitsluitend wordt vertrouwd op de techniek dient een kader te worden opgesteld dat aansluit bij de stand van de huidige wetenschappelijke aanbevelingen over de onvoorspelbare (oneerlijke en/of discriminerende) gevolgen voor betrokkenen van profilering en data-mining.

5. Te weinig harde grenzen aan toegang tot data en bestanden

Uit de MvT blijkt dat bestanden kunnen worden opgevraagd voor verkennend data-analyse-onderzoek. Uit recent onderzoek van het CTIVD blijkt dat gegevens ook van waarde kunnen zijn voor uitruil met andere diensten (*quid pro quo*). Wat door de diensten noodzakelijk wordt gevonden in het kader van opvragen gegevens en data-analyse is niet onderwerp van scherp toezicht. Het is onacceptabel dat er eigenlijk geen grenzen worden gesteld aan het verzamelen van gegevens. De grens dat het niet willekeurig dient te geschieden is geen harde grens. Willekeurigheid heeft operationeel ook geen enkele waarde voor de diensten. Wat zijn nu specifieke gevallen van dataverzameling en -analyse waarvan door de wetgever wordt gevonden dat deze niet acceptabel zijn? Het feit dat artikelen 22 en 47 eigenlijk niet aan de orde komen in de bespreking van het grondrechtelijk kader is onacceptabel.

6. Veel te smalle blik op grondrechtelijk kader

In het grondrechtelijk kader wordt voornamelijk stilgestaan bij de inbreuk op de persoonlijke levenssfeer van betrokkenen door de diensten, inclusief het recht op de bescherming van persoonsgegevens (Artikel 8 EVRM), en tot op zeker hoogte het recht op een eerlijk proces (Artikel 6 EVRM) en een effectief rechtsmiddel (Artikel 13 EVRM). Dit is onterecht. Er is, zo is algemeen geaccepteerd in de relevante literatuur over de grondrechtelijke positie van inlichtingen- en veiligheidsdiensten, ook sprake van een inbreuk op andere grondrechten, inclusief het grondrecht op vrijheid van meningsuiting, vrijheid van vereniging, het recht op gelijke behandeling (anti-discriminatie), godsdienstvrijheid, en het grondrecht op eigendom. In het bijzonder is mogelijk sprake van inbreuken op vrijheidsrechten in de publieke sfeer van personen en organisaties.

7. Slechte regeling voor bijzondere en gevoelige gegevens

De regeling voor de verwerking van bijzondere gegevens is opgenomen in Artikel 18, derde en vierde lid. Er mogen geen gegevens worden verwerkt puur vanwege deze bijzondere eigenschappen. Maar, zo blijkt uit de MvT, wat wel mag is dat dergelijke gegevens worden verwerkt als bijvoorbeeld godsdienst of levensovertuiging geldt als motivatie voor handelen dat terecht de aandacht van de diensten heeft. Maar is dat acceptabel, en hoe algemeen mag dat worden getrokken? Als specifieke mensen van een bepaalde religie bij dergelijk handelen betrokken zijn, is dan het verwerken van gegevens van deze religie in het algemeen toegestaan? Dit zou veel te kort door de bocht zijn. Gezien het door Wilders en anderen verspreide vergif over een zogenaamd inherent verband tussen de islam en geweld, is deze vraag maatschappelijk relevanter dan ooit. Een nadere reflectie op de betekenis van het begrip "onvermijdelijk" (Artikel 18, vierde lid), dat een waarborg moet vormen tegen het verwerken van bijvoorbeeld medische gegevens, is dan ook gewenst.

8. Onvoldoende handvatten voor de subsidiariteitstoets

Er is in veel gevallen sprake van samenloop van bevoegdheden om gegevens te verkrijgen. In dat geval is de gestelde regel dat de weg gekozen dient te worden die het minste nadeel oplevert voor de betrokkene(n): de subsidiariteitstoets. Maar welk kader wordt gehanteerd, om uit te maken welke weg het minste nadeel oplevert, is onduidelijk. Wordt offline verzamelen als nadeliger beschouwd dan via digitale weg, en waarom? Is observatie minder nadelig voor betrokkenen dan alles digitaal

verzamelen over een persoon of groep personen? Is het minder nadelig als gegevens worden verkregen door binnen te dringen in een automatisch werk dan deze gegevens op te vragen bij iemand die daar rechtmatig toegang toe heeft? En hoe om te gang als voor bepaalde belanghebbenden de vraag naar het nadeel verschillend uitpakt? Is het uiteindelijk niet zo dat operationele redenen voor de diensten de doorslag zullen geven? Wat komt er dan terecht van deze toets in de praktijk?