Select while you collect

Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten

Bart Jacobs[1]

In juli 2015 heeft het kabinet een voorstel geopenbaard voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv 20xx), ter vervanging van de huidige wet (Wiv 2002). De internetconsultatie over dit voorstel heeft ongebruikelijk veel reacties opgeleverd, veelal kritisch van aard, waarin bijvoorbeeld gesproken wordt van sleepnetten waarmee de diensten massaal gegevens zouden gaan verzamelen. De resultaten van deze consultatie zijn nog niet verwerkt. De twee meest controversiële onderwerpen zijn het onafhankelijke toezicht op de diensten en het interceptiestelsel. Dit artikel richt zich op het laatste onderwerp[2] en bepleit een werkwijze waarbij het verzamelen en selecteren hand in hand gaan.

In onze moderne gedigitaliseerde samenleving is het werk van de politie en van inlichtingendiensten (en hun afnemers) in hoge mate informatie-gestuurd. Niet alleen laten bijna al onze handelingen digitale sporen na – die gebruikt kunnen worden voor *a posteriori* onderzoek – maar ook kan men in bestaande sporen patronen ontdekken die a priori aanwijzingen geven voor wat nog te gebeuren staat. Met name voor inlichtingendiensten is het voorspellen en voorkomen belangrijk. Politiediensten richten zich vooralsnog vooral op bewijsverzameling, nadat de strafbare handeling reeds plaatsgevonden heeft.

Bij de grote hoeveelheden informatie die nu gegenereerd en nagelaten worden is de vraag relevant: welke informatie verzamel je, op welk moment, en op welk moment selecteer je informatie voor gebruik. Voor deze kwestie zijn de Engelse termen *select before you collect*[3] en *collect before you select* (of: *select after you collect*) in zwang geraakt.[4] De volgende twee voorbeelden illustreren het verschil.

- Politie- en inlichtingendiensten mogen de telefoongesprekken van een burger tappen wanneer de betreffende persoon als verdachte of *target* aangemerkt is,[5] en een hogere autoriteit toestemming heeft gegeven voor de tap – de rechter-commissaris bij de politie, of de minister bij de inlichtingendiensten. De gesprekken worden dus pas verzameld nadat een verdachte geselecteerd is. Hier geldt: *select before you collect.*
- De Europese Dataretentierichtlijn (06/24/EG) uit 2006, in Nederland sinds 2009 van kracht als de Wet bewaarplicht telecommunicatiegegevens, verplicht aanbieders van telefoon en internet ertoe de metadata van al hun klanten te bewaren. Deze metadata betreffen welk nummer of adres op welk moment (waar) met welk ander nummer/adres belt of mailt, en wie op welk moment met welk IP-adres in- of uitlogt.[6] In dit voorbeeld geldt: *collect before you select*, omdat van iedereen gegevens verzameld worden en pas later geselecteerd wordt van wie gegevens eventueel gebruikt worden.

Deze bewaarplicht is van begin af aan omstreden geweest vanwege het bij voorbaat verzamelen van informatie over meestal onverdachte burgers. Het Duitse Constitutionele Hof heeft de richtlijn al in 2009 een schending van het (Duitse) grondrecht op privacy genoemd. In 2015 heeft het Europese Hof van Justitie de richtlijn in de gehele unie ongeldig verklaard: 'Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke.' (ECLI:EU:C:2014:238, punt 65). De interpretatie van deze laatste opmerking in de context van dit artikel is: er wordt te veel verzameld en te weinig geselecteerd.

Het is evident niet proportioneel wanneer van de gehele bevolking alle communicatie-metadata opgeslagen worden, terwijl slechts een fractie daarvan daadwerkelijk gebruikt wordt. Voorstanders van dataretentie bagatelliseren de privacyschending door te zeggen dat er toch niets aan de hand is als gegevens helemaal niet gebruikt worden. Dit is een merkwaardig argument; dat het ophangen van een camera in ieders slaapkamer rechtvaardigt, zolang

er maar niks met de opnames gedaan wordt. Het simpele feit dat gegevens opgeslagen worden, en mogelijk gebruikt, gelekt, of gehackt worden, heeft een *chilling effect*, waardoor mensen bijvoorbeeld terughoudend zijn om met een psychiater te bellen, of met familie in Pakistan.

De onderliggende fundamentele kwestie is of je het verzamelen van gegevens moet reguleren, of het gebruik ervan moet reguleren. Deze kwestie hangt nauw samen met het verschil tussen *select before you collect* en *collect before you select*. De *collect before you select* aanpak is alleen dan te rechtvaardigen wanneer een groot deel van wat verzameld wordt ook daadwerkelijk gebruikt wordt. De *select before you collect* aanpak veronderstelt dat je van te voren precies weet waar je naar op zoek bent. Dat is in een inlichtingen context niet altijd het geval. Daarom is de hieronder voorgestelde tussenvorm – *select while you collect* – relevant.

Voorbeeld 1. Wanneer een inlichtingendienst eenmaal toestemming gekregen heeft om de telefoon van een doelwit te tappen, krijgt de telecomprovider van het doelwit de opdracht om alle gesprekken rechtstreeks door te sturen naar de dienst. Ook dan speelt weer de kwestie van de verhouding tussen verzamelen en gebruik (in de vorm van daadwerkelijk beluisteren)[7] van getapte gesprekken. Het is in de context van dit artikel zeer relevant dat de toezichthouder – de Commissie voor Toezicht op de Inlichtingen- en Veiligheidsdiensten CTIVD – daadwerkelijk ingrijpt en aanbeveelt taps stil te leggen wanneer talrijke gesprekken wel getapt (verzameld) worden maar niet beluisterd (geselecteerd) worden. Dit kan bijvoorbeeld het geval zijn bij capaciteitsproblemen (gebrek aan vertalers) of bij hogere prioriteiten van ander onderzoek. Dit ingrijpen vindt niet plaats op basis van een specifieke bepaling in de Wiv, bijvoorbeeld over bewaar- of vernietigingstermijnen, maar op basis van proportionaliteit en noodzakelijkheid.

Enige achtergrondinformatie over interceptie

De interceptiebepalingen in de Wiv 2002 zijn techniekafhankelijk geformuleerd: de toegang van de diensten tot communicatie is afhankelijk van de manier van overbrenging. Informatie door de lucht mag zonder last ongericht, *in bulk* worden opgevangen voor een doel in relatie tot de taken van de diensten (zie art. 12 Wiv 2002), terwijl het verzamelen van informatie die via een kabel (bijvoorbeeld koper of glasvezel) verstuurd wordt, alleen gericht op een zeer specifiek doelwit (persoon of organisatie), met een last van de verantwoordelijke minister, toegestaan is. Het kabinet wil dit merkwaardige onderscheid tussen ether en kabel, en daarmee ook het onderscheid tussen wel-of-niet ongerichte interceptie, in navolging van de commissie Dessens, opheffen, en tegelijkertijd een nieuw stelsel van waarborgen invoeren.[8] De huidige Wiv 2002 vereist een last van de verantwoordelijke minister voor het zoeken naar 'kenmerken' in de opgevangen niet-kabelgebonden informatie. Beperkingen bestaan er voor de toegang tot deze verzamelde informatie. Om een simpel beeld te gebruiken: men laat een grote bak vollopen, maar beperkt waarnaar gevist mag worden in deze bak. Hier is sprake van eenzelfde gebrek aan proportionaliteit als bij de eerder besproken, buiten werking gestelde, Europese Dataretentie-richtlijn.

Vraag. Waarom legt de CTIVD wel een proportionaliteits- en noodzakelijkheidseis op bij het verzamelen van telefoontaps, zoals beschreven in Voorbeeld 1, maar wordt de evident niet-proportionele bulk verzameling van niet-kabelgebonden informatie ongemoeid gelaten? Aan deze zaken wordt op verschillende manieren aandacht gegeven. Dit wordt ook met zoveel woorden toegegeven. Het belang van deze vraag neemt toe bij de nieuwe voorgestelde bevoegdheden, bijvoorbeeld omdat de commissie Dessens pleit voor gelijktijdige versterking van de waarborgen.

Dit is een merkwaardig argument; dat het ophangen van een camera in ieders slaapkamer rechtvaardigt zolang er maar niets met de opnames gedaan wordt

Bij communicatie kan onderscheid gemaakt worden tussen inhoud en metadata. De inhoud betreft bijvoorbeeld wat er feitelijk in een email staat, of wat er over de telefoon besproken wordt. Metadata kan men beschouwen als informatie over de communicatie, bijvoorbeeld het adres (mail, IP, MAC) of telefoonnummer of het tijdstip of de locatie van communicatie. Traditioneel wordt inhoud als privacy-gevoeliger gezien dan metadata, en daarom beter

Auteur

1. Prof. dr. B.P.F. Jacobs is hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen. Daarnaast is hij lid van de Cyber Security Raad en van de Kennis Kring van de CTIVD en zit hij de Raad van Advies van Bits of Freedom voor. Dit artikel is een uitwerking en actualisering van de *NJB*-blog 'Vluchtig en Stelselmatig. Een bespreking van interceptie door inlichtingen- en veiligheidsdiensten', 5 februari 2015.

Noten

2. Voor meer informatie en discussie over de bevoegdheden van de toezichthouder, zie: J.P. Loof et al, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Leiden: Universiteit Leiden 2015, en ook: S. Eskens et al, *Ten standards for oversight and transparency of national intelligence services*, Amsterdam: Universiteit Amsterdam 2015.

3. B. Jacobs, 'Select before you Collect', *Ars Aequi*, jaargang 54, december 2005, p. 1006-1009.

4. Het begrip 'selecteren' heeft in de context van de WIVD een heel eigen betekenis, namelijk het onderzoeken van de inhoud van communicatie. Hier wordt het begrip echter in algemene zin gebruikt, als 'uitkiezen'.

5. Verkennend onderzoek wordt hier voor het gemak buiten beschouwing gelaten.

6. De koppeling van deze nummers/adressen aan specifieke personen vergt een aparte stap, die in een buitenlandse context aanzienlijk moeilijker is dan in een binnenlandse.

7. Of 'uitluisteren' zoals het in deze sector vaak met een lelijk woord genoemd wordt.

8. *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, december 2013.

beschermd. Volgens de huidige Wiv mogen de diensten metadata van ongericht opgevangen niet-kabelgebonden communicatie zonder last verzamelen. Metadata kunnen echter ook veel onthullen, niet alleen in isolatie (wat zegt het feit dat u gebeld heeft met een abortuskliniek?), maar zeker in onderlinge combinatie. De moderne mens maakt op velerlei manieren gebruik van elektronische communicatiemiddelen en diensten en laat daarmee een onthullend spoor van metadata achter. Na een verhelderend artikel[9] in *De Correspondent* begrijpt iedereen dat systematisch vergaren van metadata betere bescherming verdient, en dat er geen groot onderscheid in privacygevoeligheid meer is tussen stelselmatige metadata verzameling en kennisneming van de inhoud van communicatie. Het Wiv-voorstel kent het onderscheid tussen inhoud en metadata, zie artikel 35, waar metadata omschreven worden als 'gegevens anders dan die welke de inhoud van de desbetreffende telecommunicatie betreft'. Waar het gaat om metadata-analyse die inbreuk maakt op de privacy wordt toestemming van de betrokken minister noodzakelijk (artikel 35 lid 2).

Inlichtingen- en veiligheidsdiensten maken intensief gebruik van metadata voor wat heet *traffic-analysis:* wie communiceert met wie, wanneer, waar en hoelang en met welke *identifiers*. Hiermee kan een *social graph* gemaakt worden die bijvoorbeeld een beeld geeft van een terroristische of andere groepering.

De moderne mens maakt op velerlei manieren gebruik van elektronische communicatiemiddelen en diensten en laat daarmee een onthullend spoor van metadata achter

Een belangrijk, controversieel punt betreft zogenaamde 'historische metadata': het in *bulk* verzamelen van metadata voor later gebruik, voor (nu) onbekende doelwitten, bijvoorbeeld om achteraf terug te kunnen zoeken na een aanslag. Diensten stellen dat dit van groot belang is voor hun effectiviteit, maar zulk in *bulk* verzamelen, en het nut ervan, is zeer omstreden, waarbij de fundamentele vraag is of de opbrengst opweegt tegen de inbreuken. De Amerikaanse *Privacy and Civil Liberties Oversight Board* (PCLOB) schrijft in haar rapport van januari 2014:[10] 'The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government ends the program.' In diezelfde maand heeft president Obama in zijn *Presidential Policy Directive 28 – Signals Intelligence Activities*[11] in-bulkverzameling door de Amerikaanse inlichtingendiensten weliswaar in stand gehouden, maar het gebruik ervan beperkt tot bepaalde doelen (contraspionage, -terrorisme en -proliferatie van massa vernietigingswapens, verdediging tegen cyber dreigingen, tegen eigen militairen en bondgenoten, en internationale misdaad) en het gebruik voor specifieke andere doelen uitgesloten (zoals onderdrukking van kritiek, discriminatie, of economische spionage). Dergelijke themagerichte bepalingen ontbreken in de Nederlandse wet. Echter nu, na een door het Amerikaanse Congres in juni 2015 goedgekeurde hervorming, heeft de NSA sinds eind november 2015 niet langer de bevoegdheid om zelf (telefoon) bulk-metadata van Amerikanen te verzamelen.[12] Deze gegevens worden nu door de Amerikaanse telefoonmaatschappijen verzameld en mogen alleen nog gericht, na toestemming van een rechter, door de NSA opgevraagd worden. Kennelijk volstaat gerichte toegang en is grootschalige netwerkanalyse minder belangrijk, althans voor binnenlands gebruik.

Terzijde: In dit artikel staat interceptie centraal. Dit betreft het opvangen van communicatie die 'in transit' is tussen twee of meerdere partijen. Traditioneel is interceptie een van de belangrijkste bronnen van informatie voor een inlichtingendienst. Voor een deel blijft dat zo, maar het belang en de opbrengst van interceptie nemen af, door toenemend gebruik van sterke *(end-to-end)* versleuteling, door grotere variatie in communicatiemiddelen (bijvoorbeeld communicatie via spelcomputers), en door grotere mobiliteit van gebruikers. Een van de *eye-openers* van de Snowden-onthullingen is de omvang en het belang van computerinbraak-operaties in het moderne inlichtingenwerk. Hierbij wordt op de computer van een target ingebroken, om daar de gezochte informatie rechtstreeks op te halen, nog voordat sprake is van versleutelde communicatie. De NSA spreekt van *end-point-operations* of van *computer-network-exploitation*. Binnen de in 2014 door de AIVD en MIVD gezamenlijk opgerichte *Joint Sigint Cyber Unit* (JCSU) zijn ook Nederlandse specialisten op dit gebied actief. Het Wiv 20xx voorstel heeft enigszins aangepaste bepalingen op dit gebied (artikel 30) ten opzichte van de Wiv 2002 (artikel 24); zie de reactie van de CTIVD, sectie 3.5, voor een bespreking.[13]

Overigens willen de Nederlandse diensten toegang tot de kabel voor nog een andere activiteit, namelijk het defensief monitoren van computernetwerken om digitale aanvallen te detecteren. Omdat het netwerkverkeer hierbij slechts snel en vluchtig doorzocht wordt om patronen te herkennen is hierbij in beginsel geen sprake van interceptie en blijft deze activiteit hier verder buiten beschouwing.

Het voorstel voor een nieuwe Wiv

In het wetsvoorstel Wiv 20xx zijn de artikelen 31 t/m 35 gewijd aan interceptie. Het voorstel beschrijft, in navolging van de commissie Dessens, een driefasenmodel, bestaande uit de fasen van verwerving, voorbewerking, en verwerking. Verwerving verwijst naar de interceptie zelf. Voorbewerking verwijst naar het bepalen van het juiste interceptiekanaal (frequentie, kabel, vezel) en het zo nodig of zo mogelijk ontsleutelen van de opgevangen communicatie. Deze activiteit van het bepalen van het juiste kanaal

wordt ook aangeduid met 'search gericht op interceptie' (artikel 34 lid 1). Verwerking van de onderschepte gegevens kan verschillende activiteiten omvatten, zoals statistische analyse van metadata (artikel 35 lid 2), of het uitproberen van kenmerken en het zoeken naar nieuwe doelwitten, ook wel genoemd 'search gericht op selectie' (artikel 34 lid 2). De daadwerkelijke kennisneming en gebruik van de inhoud ('selectie' in de terminologie van de Wiv) van communicatie mag alleen gericht plaatsvinden (op basis van artikel 32), wanneer sprake is van een specifiek doelwit (persoon of organisatie).[14]

In haar reactie op het wetsvoorstel bespreekt de CTIVD – ondersteund door een verhelderend schema – dit driefasenmodel in detail, gebaseerd op haar ervaring met de praktijk van de diensten. De CTIVD benadrukt dat deze drie fasen niet sequentieel maar parallel begrepen moeten worden en dat terugkoppelingen een belangrijke rol spelen om de gerichtheid van de interceptie te verbeteren. Voorts doet de CTIVD enkele voorstellen tot verheldering van deze interceptieartikelen.

9. D. Tokmetzis, 'Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst', *De Correspondent* 20 december 2013.

10. Volledige titel: Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court.

11. Zie: www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

12. Aan de bevoegdheid om gegevens van niet-Amerikanen te verzamelen verandert niets.

13. Reactie CTIVD op concept-wetsvoorstel Wiv 20xx, 26 augustus 2015. Beschikbaar via www.ctivd.nl.

14. Art. 34 Wiv 20xx staat wel toe dat (kortstondig) kennis genomen wordt van de inhoud maar alleen ten behoeve van search gericht op selectie. Dit verschilt van daadwerkelijke kennisneming en gebruik, zoals bij het beluisteren van een gesprek of bestuderen van een email in een onderzoek (art. 32).

De aandacht richt zich hier niet zozeer op de precieze formulering van deze bepalingen, maar op het onderliggende model. Ook in de nieuw voorgestelde wet wordt uitgegaan van *collect before you select*, waarbij geïntercepteerde gegevens in een grote bak terechtkomen en daarin drie jaar lang bewaard mogen blijven. De beperkingen die de wet stelt richten zich op de soorten onderzoek die op deze bak uitgevoerd mogen worden. De omvang van de bak hoeft niet beperkt te worden, en niet-relevante inhoud hoeft niet per ommegaande verwijderd te worden. Ter vergelijking: een van de onthullingen van Edward Snowden betreft het zogenaamde *Xkeyscore* programma van de Amerikaanse NSA en Britse GCHQ waarbij op grote internetknooppunten in de wereld alle gegevens verzameld worden. Dit programma is vanwege zijn omvang bekritiseerd maar kent wel een *rolling buffer*. Daarbij worden de verzamelde gegevens na enige tijd automatisch overschreven door wat nieuw binnenkomt. De overschrijvingstermijn is 3-5 dagen voor inhoud, en circa 30 dagen voor metadata. Binnen deze periode zal relevantie vastgesteld moeten worden en zullen kopieën gemaakt moeten worden voor eventuele langduriger opslag.

Werkwijze gebaseerd op select while you collect

Zoals hierboven reeds genoemd veronderstelt de *select before you collect* aanpak dat van te voren bekend is waarnaar gezocht wordt – hetgeen in de wereld van inlichtingen- en veiligheidsdiensten niet realistisch is.

Voorbeeld 2. Stel een Nederlandse inlichtingen en veiligheidsdienst ontvangt een bericht van een buitenlandse partnerdienst dat een bepaald individu in Nederland mogelijk gevaarlijke plannen heeft. Op basis hiervan wordt een onderzoek gestart. Uit verkenningen blijkt dat het individu in kwestie – zeg Harry, voor het gemak – altijd communiceert via het draadloze wifi-netwerk in de trein. Nu zou de NS opgedragen kunnen worden al het internetverkeer uit de trein door te geleiden naar de dienst, zodat in al die gegevens gezocht kan worden naar de communicatie van Harry. Deze aanpak volgt het model waarbij een grote bak vol stroomt waarin onder voorwaarden gezocht kan worden. De voorwaarden betreffen de kenmerken waarmee men de communicatie van Harry probeert te vinden. Is deze werkwijze, waarbij van alle – meer dan een miljoen – dagelijkse treinreizigers al het internetverkeer in de trein voor drie jaar bewaard wordt, noodzakelijk, proportioneel en subsidiair? Het antwoord is duidelijk nee! Dit zal ook onder de nieuwe Wiv niet toegestaan zijn.

Terzijde: een proportioneel en subsidiair alternatief is het volgende. Een medewerker van de dienst gaat in de trein vlakbij Harry zitten en zet daar een nepwifi aan, ook met naam 'WiFi in de trein', maar met een sterker signaal. De computer (of telefoon of tablet) van Harry zal vervolgens vanzelf met dat sterkere netwerk verbinden, waarmee identificerende kenmerken (zoals het MAC adres) van de apparatuur van Harry verkregen en herkend kunnen worden. Vervolgens kan de NS opgedragen worden om (alleen) al het verkeer gerelateerd aan dit adres aan de dienst door te geleiden. Het gaat dan om een gerichte tap.

Voorbeeld 3. We veranderen het tweede voorbeeld enigszins: Harry communiceert nu niet vanuit de trein, maar vanuit een bepaald internetcafé, met dagelijks een honderdtal bezoekers. Laten we er even van uit gaan dat de zojuist beschreven nepwifi truc niet werkt, bijvoorbeeld omdat Harry via een daar opgestelde vaste computer werkt, en ook dat andere acties uitgesloten zijn, bijvoorbeeld omdat men de uitbaters van het internetcafé niets wil laten blijken van de belangstelling voor Harry. De dienst overweegt dus het hele café te tappen. Is het drie jaar lang opslaan van alle communicatie van alle bezoekers van het café in dit geval te rechtvaardigen? De 'grote bak' systematiek van de (huidige en nieuwe) Wiv regelt dat er in al die gegevens van al die andere bezoekers slechts gezocht mag worden naar kenmerken van Harry.

Aan de hand van dit voorbeeld laat de *select while you collect* systematiek zich goed illustreren. Bij die aanpak gaan het verzamelen en het selecteren (of preciezer: het 'searchen') hand in hand. Direct bij het verzamelen worden irrelevante zaken na vluchtige inspectie weggegooid, zoals alle YouTube filmpjes, tenzij ze van bijzondere aard zijn (bijvoorbeeld onthoofdingen of bomhandleidingen). Zaken die wel relevant lijken kunnen apart gezet worden, en in een volgende, minder vluchtige analyse, alsnog beoordeeld worden op mogelijke relevantie voor het onderzoeksdoel (de communicatie van Harry vinden en bekijken). Indien deze interceptie gecombineerd wordt met observatie kan sowieso al het getapte verkeer onmiddellijk weggegooid worden wanneer Harry niet aanwezig is in het café. En wanneer hij er wel is kan bijvoorbeeld geconstateerd worden dat er juist dan versleutelde email verstuurd wordt of een VPN-verbinding opgezet wordt. Dit kan aanknopingspunten leveren voor verder onderzoek, waarbij de tap van het internetcafé steeds gerichter uitgevoerd kan worden.

De grootste moeilijkheid lijkt te zijn dat de *select while you collect* aanpak zeer dynamisch is en zich daarmee moeilijk in een statische wet vast laat leggen

Uit geluiden vanuit de Nederlandse diensten blijkt dat deze *select while you collect* systematiek is wat men wil gebruiken, niet alleen omwille van privacybescherming, maar ook omwille van efficiëntie en het voorkomen van ruis. Waarom is de nieuwe wet dan niet volgens die systematiek geschreven? Er wordt gesproken over 'technische verkenning', 'technische analyse' en 'optimalisatie van de uitoefening' maar deze technieken zijn ogenschijnlijk niet gericht op de bescherming van de persoonlijke levens-

sfeer. De grootste moeilijkheid lijkt te zijn dat de *select while you collect* aanpak zeer dynamisch is en zich daarmee moeilijk in een statische wet vast laat leggen. Misschien wil je wel 99,99% van een bepaalde tap binnen een seconde weggooien, en wil je maar het hele kleine resterende deel langer bewaren. Hoe leg je dat vast? De wet zal zich richten op de uiterste bewaartermijnen. De toezichthouder is echter beter in staat om te gaan met dit dynamische karakter en kan hierbij een nadrukkelijker rol spelen, in lijn met de werkwijze met betrekking tot telefoontaps uit Voorbeeld 1: wanneer verzamelde gegevens niet gebruikt worden kan de toezichthouder opdracht geven tot vernietiging.

Om de werkwijze van de diensten toch nadrukkelijker volgens deze *select while you collect* systematiek als waarborg te laten verlopen volgt hier een drietal suggesties:

1) In het eerste (niet-specifieke) interceptieartikel (nummer 33 in het voorstel) wordt de voorwaarde van proportionaliteit en noodzakelijkheid (nogmaals) expliciet benadrukt.
2) *Select while you collect* wordt expliciet beschreven als beoogde werkwijze in de memorie van toelichting van het uiteindelijke wetsvoorstel – in contrast met de 'grote bak' systematiek van *collect before you select*.
3) De toezichthouder hanteert deze *select while you collect* werkwijze als maatstaf voor het toezicht op interceptie – in lijn met de bestaande aanpak met betrekking tot telefoontaps uit Voorbeeld 1.

De CTIVD heeft eerder aangegeven het toezicht meer te willen automatiseren. Dat zou bijvoorbeeld kunnen door van de diensten per onderzoek een automatisch gegenereerd overzicht te vragen van welk percentage van de geïntercepteerde gegevens na hoeveel tijd verwijderd is, en op basis van welke kenmerken. Zulke percentageoverzichten zouden zelfs gepubliceerd kunnen worden. Dit kan een wezenlijke invulling zijn van de versterking van de waarborgen die volgens het kabinet (in navolging van de commissie Dessens) hoort bij de uitbreiding van de bevoegdheden van de diensten.

Tot slot nog een drietal overwegingen. Ten eerste, men zou kunnen tegenwerpen dat de *select while you collect* systematiek niet stringent genoeg is en te veel ruimte laat aan medewerkers van de dienst. Positiever geformuleerd kan men zeggen dat de systematiek een beroep doet op hun verstandigheid (de Aristotelische deugd fronèsis),[15] hier begrepen als combinatie van vakkennis en moreel besef. Juist deze dienst-medewerkers, die opereren aan de rafelranden van de maatschappij, dienen goed getraind te zijn in zulke verstandigheid. In de dynamische, snel veranderende wereld van ICT heeft een welbegrepen flexibele regel meer waarde dan een starre wet die alleen uitersten regelt.

Ten tweede geven de genoemde voorbeelden (noodzakelijkerwijs) slechts een beperkt beeld: ze zijn *target-centric*, waarbij het doelwit al bekend is, in een binnenlandse situatie. Juist binnen Nederland is er sprake van een uitgebreide veiligheidsketen waardoor er een breed spectrum aan meer en minder ingrijpende (bijzondere) bevoegdheden beschikbaar is. Zulke alternatieven zijn in een buitenlandse context vaak afwezig, waardoor de toets van proportionaliteit en subsidiariteit daar een andere invulling heeft. Verschillende landen kennen zelfs aparte diensten voor nationale en internationale inlichtingenactiviteiten. Nederland kent echter zo'n nationaal-internationaal onderscheid niet, noch voor de bevoegdheden en noch voor de waarborgen. Bij een versterking van de waarborgen zal deze uniforme benadering onder druk komen te staan.

Ten slotte, de discussie over het belang van historische metadata blijft bestaan. Meer inzicht in het belang en het gebruik van niet-direct nuttige gegevens ('in de grote bak') is van belang voor de publieke discussie. Na een aanslag zoals in november 2015 in Parijs verspreiden de Franse diensten direct *identifiers*, zoals telefoonnummers en andere contactgegevens, onder collegadiensten, die vervolgens op zoek gaan naar mogelijke aanknopingspunten (via *call chaining*) in hun eigen opgeslagen gegevens. Dit kan belangrijke aanwijzingen geven. Maar hoeveel gegevens moet je voor dit soort gelegenheden verzamelen? In theorie alles. Maar wat is in de praktijk nuttig, noodzakelijk en proportioneel? De hier voorgestelde *select while you collect* werkwijze gaat niet samen met het blind opslaan van grote hoeveelheden gegevens voor mogelijk later gebruik. Bij het opvangen wordt na een vluchtige analyse de relevantie beoordeeld. Hier schuilt een wezenlijke beperking van de werkwijze: de beoordeling kan slechts één keer op één wijze plaatsvinden, want eenmaal weggegooide gegevens zijn weg. Hoe sterk is deze beperking? Aan welke knoppen kan gedraaid worden om tot afweging van belangen te komen? Onafhankelijk onderzoek naar deze materie zou helderheid kunnen verschaffen. In de huidige constellatie is alleen de toezichthouder CTIVD daartoe in staat, omdat universitaire onderzoekers in beginsel geen toegang hebben tot de (geheime) opgeslagen gegevens van de diensten. Zulk onderzoek wijkt enigszins af van het meer operationeel gerichte onderzoek dat de toezichthouder gewoon is uit te voeren. Hopelijk is er desondanks ruimte voor te maken. Het draagt bij aan een debat dat op feiten gebaseerd is. •

In de dynamische, snel veranderende wereld van ICT heeft een welbegrepen flexibele regel meer waarde dan een starre wet die alleen uitersten regelt

15. Zie bijv. M. Becker, P. van Tongeren, A. Hoekstra, E. Karssing & R. Niessen. *Deugdethiek en integriteit. Achtergronden en aanbevelingen*, Assen: Van Gorcum 2010.