Prof. dr. B.P.F. Jacobs en dr. W.G. Teepe[1]

Over vermogen en onvermogen

186

Trefwoorden:
informatietechnologie, stemcomputers, computerbeveiliging, databases, privacyinbreuken

De inzet van moderne informatietechnologie voor cruciale taken van de overheid, zoals het organiseren van verkiezingen en het bewaren van veiligheid en privacy van burgers, zonder adequate regelgeving en controle biedt betrokken partijen ruime vrijheid van handelen. Dit wordt geconstateerd aan de hand van drie rapporten. Daarbij blijken burgers enerzijds afhankelijk te zijn van het vermogen van betrokken partijen tot zelfbeperking om misbruik van de beschikbare ruimte te voorkomen. Anderzijds geeft geconstateerd onvermogen om effectief met deze ruimte tot het vergaren en verwerken van gevoelige gegevens om te gaan tot nu toe enige mate van garantie tegen oneigenlijke inbreuken.

1 Informatie ter discussie

Deze bespreking betreft drie verschillende rapporten die dit jaar verschenen zijn. De achtergrond van deze rapporten is totaal verschillend en ongerelateerd. Toch is er, van enige afstand bezien, een overeenkomst waar te nemen. Alle drie betreffen ze de omgang van de overheid met informatietechnologie (IT) in relatie tot basiswaarden als privacy, veiligheid en democratie. Een moderne overheid maakt immers uitgebreid gebruik van IT in gevoelige processen zoals surveillance, het beheren van persoons- en gedragsgegevens van burgers en de verwerking van uitgebrachte stemmen.

Het meest recente van de drie rapporten is de conceptversie van *Data voor Daadkracht*[2] (in het vervolg *D4D*), waarin onderzocht wordt welke systematiek er bij de diensten in het veiligheidsdomein (zoals AIVD, politie en de bijzondere opsporingsdiensten) bestaat voor het inwinnen en uitwisselen van gegevens uit externe databases. De belangrijkste bevindingen van dit rapport zijn eenvoudig samen te vatten: er is geen eenduidige systematiek hiervoor, en de noodzaak daartoe wordt ook niet breed ervaren. De informatiehuishouding in het veiligheidsdomein is versnipperd en verkokerd.

Daarnaast is er het rapport *Van privacyparadijs tot controlestaat?*[3] (in het vervolg *PP2CS*), waarin de juridische kaders voor het inwinnen van privacygevoelige gegevens door de overheid in kaart worden gebracht. De belangrijkste bevinding is dat de bevoegdheden van de diensten in het veiligheidsdomein in de afgelopen jaren sterk verruimd zijn, zonder dat er ooit een maatschappelijke discussie is gevoerd over het cumulatieve effect van alle bevoegdheden.

Veel media-aandacht is uitgegaan naar het onderwerp van het derde rapport, *Stemmachines, een verweesd dossier*[4] (in het vervolg *S1VD*), waarin onderzocht is hoe de overheid gedurende de afgelopen decennia is omgegaan met stemcomputers en met de bijbehorende betrouwbaarheidseisen. Het rapport schetst een beeld van een overheid die tot voor kort vrijwel geen aandacht schonk aan de IT-aspecten (met name beveiliging) van stemcomputers en aan waarschuwende signalen dienaangaande.

Welk beeld rijst op uit deze drie rapporten? Op welke wijze wordt omgegaan met de basiswaarden van veiligheid (*D4D*), privacy (*PP2CS*) en democratie, in het bijzonder stemmen (*S1VD*)? Het antwoord op deze vragen is voor een groot deel juridisch (welke regelgeving is er) maar zal hier benaderd worden vanuit de specifieke achtergrond van de auteurs op het gebied van computerbeveiliging en privacy.

2 De overeenkomsten tussen de drie rapporten

Er is een grote hoeveelheid wet- en regelgeving die gaat over het beheren van persoonsgegevens. Het interpreteren en implementeren daarvan is geen sinecure. Laten we kijken wat de verschillende rapporten over dit beheer te melden hebben.

2.1 *D4D*

In de samenvatting van *D4D* valt te lezen:[5]

> '6. Er bestaat geen totaaloverzicht van de bestaande wet- en regelgeving met betrekking tot het inwinnen van gegevens uit externe databases. Het is niet mogelijk om inzicht te verkrijgen in consistentie en samenhang van deze wet- en regelgeving.'

En even verderop:[6]

> '18. Aan te stellen normen op het gebied van de grondslag en de vormvereisten wordt niet voldaan, omdat onvoldoende inzicht bestaat in de toepasselijke wet- en regelgeving, de mate waarin inlichtingen- en opsporingsdiensten zich houden aan de geldende regels en omdat de afscherming van de bevraging voor onbevoegden onvoldoende kan worden verzekerd.'
>
> '19. Aan te stellen normen op het gebied van maatschappelijke zorgvuldigheid wordt niet voldaan omdat onvoldoende inzicht bestaat in proportionaliteit en sub-

---

1 **Bart Jacobs en Wouter Teepe zijn verbonden aan de Security of Systems groep van de Radboud Universiteit Nijmegen, en beiden betrokken bij het Centre for Cybercrime Studies (Cycris).**

2 H. Bosma e.a., *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*, Den Haag: Adviescommissie Informatiestromen Veiligheid 2007 (conceptversie).

3 A. Vedder e.a., *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw (Study 49)*, Den Haag: Rathenau Instituut 2007.

4 L.M.L.H.A. Hermans & M.J.W. van Twist, *Stemmachines, een verweesd dossier*, Den Haag: Commissie Besluitvorming Stemmachines 2007.

5 *D4D*, p. 10.

6 *D4D*, p. 11.

sidiariteit en omdat een afdoende inzicht in het aantal bevragingen en de groei daarin ontbreekt. …'

Het rapport stelt dat er overheidsbreed te weinig moeite wordt gedaan om verantwoording af te leggen over het gebruik van (persoons)gegevens. Er wordt *niet* op voorhand gesteld dat het onmogelijk zou zijn om overtuigende verantwoording af te leggen, er wordt niet gesuggereerd dat er onbillijke zaken zouden gebeuren in het desbetreffende domein. Wel worden er vraagtekens geplaatst bij de grote groei in het aantal bevragingen (van externe databases) waarvoor niemand een echte verklaring heeft. Het rapport geeft mede daarom de voorvechters van burgerrechten gelijk op het punt dat er te weinig inzicht wordt gegeven in, en verantwoording wordt afgelegd over, de mate van privacyschending door opsporings- en veiligheidsdiensten.

2.2 *PP2CS*

In *PP2CS* wordt een beeld gegeven van de ontwikkeling van de privacywetgeving van 1960 tot 2006. Het algemene beeld is dat sinds de jaren negentig het geheel aan Nederlandse wetgeving steeds meer inbreuken op de privacy toestaat. De gebeurtenissen op 9/11 hebben dit wel enigszins versneld, maar zijn zeker niet de oorzaak of het begin van deze trend.

PP2CS heeft veel stof doen opwaaien en veel weerstand gekregen. Kenmerkend voor die weerstand is bijvoorbeeld dat Harm Brouwer, voorzitter van het college van procureurs-generaal, het rapport afdoet als een 'partij doemdenken' en in feite een beroep doet op vertrouwen in de gepastheid van beslissingen van het Openbaar Ministerie. Brouwer weigert inzage te geven in, of verantwoording af te leggen over, de criteria voor inbreuken op de privacy, zoals het leggen van een telefoontap.[7]

Gezien zulke weerstand tegen de boodschap van *PP2CS* is het belangrijk goed te begrijpen wat er wél en wat er niet in *PP2CS* staat. Het rapport probeert vooral een inventarisatie te geven van alle informationele bevoegdheden die in de afgelopen jaren zijn toebedeeld aan verschillende overheidsdiensten. De auteurs van het rapport maken zich zorgen over het feit dat er nooit een fundamentele discussie over het gezamenlijke effect van de vele bevoegdheden is gevoerd: 'Vooral wordt echter duidelijk dat de optelsom van maatregelen zorgwekkende gevolgen heeft voor de privacy van de doorsnee burger.'[8] Maar wat er niet in het rapport staat, is of er ook daadwerkelijk ten volle gebruik gemaakt wordt van de bevoegdheden. En wat ook niet in het rapport staat is of de gegevens die met deze bevoegdheden verzameld zijn ten volle benut worden, of alle mogelijke technieken tot het koppelen van deze gegevens effectief toegepast worden.

Kortom, *PP2CS* is primair een juridische inventarisatie met als grove conclusie dat de overheid 'bijna alles mag'. Er staat *niet* dat alles wat mag, ook daadwerkelijk gebeurt. Er staat *wel* dat het niet zeker is dat alles wat niet mag ook niet gebeurt; we weten niet of de overheidsdiensten zich aan de regels houden.[9]

> 'Wat echter opvalt … is dat … de waarborgen voor een zorgvuldige omgang met de gegevens weinig zijn uitgewerkt. En voor zover deze waarborgen al bestaan, worden ze amper nageleefd.'

Met de waarborgen die amper worden nageleefd wordt met name gedoeld op de notificatieplicht. Op basis van het bovenstaande kunnen we concluderen dat er inmiddels een situatie bereikt is waarin de overheid (met name de opsporingsdiensten) de bevoegdheid heeft om bij vrijwel alle (veelal digitale) gegevens te kunnen komen die over u en mij opgeslagen liggen. Dit pleit is beslecht.

2.3 *SIVD*

Het rapport *S1VD* behandelt een ander, meer gerelateerd onderwerp, namelijk hoe er wordt omgegaan met het vertrouwen van burgers in verkiezingsuitslagen. Het stemgeheim is een speciaal privacyrecht. Dat uitgebrachte stemmen op de juiste manier vertaald worden in een verkiezingsuitslag is een cruciaal onderdeel van de democratie.

S1VD vertelt het relaas van hoe stemcomputers eind jaren tachtig en begin jaren negentig van de vorige eeuw zonder noemenswaardig publiekelijk debat hun intrede hebben gedaan in het stemproces, en hoe deze systemen na vele jaren van gebruik niet bleken te voldoen vereisten van controleerbaarheid. Zo is bijvoorbeeld een betekenisvolle hertelling van stemmen onmogelijk.[10] Ook blijkt dat dergelijke te verwachten vereisten niet vertaald zijn in vereisten aan de infrastructuur voor het uitvoeren van verkiezingen. Het rapport constateert:[11]

> 'b) het ontbreken van een inhoudelijk programma van eisen voor alle in het verkiezingsproces betrokken apparatuur en software (anders dan het nabootsen van het stemmen met stembiljet en potlood);'
> en:
>
> 'e) het niet aan een goedkeuringsprocedure onderwerpen van de uitslagberekeningsprogrammatuur (het Integraal Stem Systeem);'

Het rapport heeft kritiek op veel van de betrokken partijen, waaronder de overheid in verschillende hoedanigheden, TNO en Groenendaal Bureau voor Verkiezingsuitslagen. Er wordt echter *niet* gesteld dat er verkiezingen zijn geweest waarbij het ook echt is misgegaan: dat er gesjoemeld zou zijn met de uitslag, of dat er daadwerkelijk ingebroken zou zijn op het stemgeheim van kiezers. Er wordt *wel* gesteld dat de garanties voor controleerbare, geheime verkiezingen aan een grondige herziening toe zijn, en vragen om politieke sturing en aandacht. Niet voor niets is dan ook gekozen voor de titel 'Stemmachines, een verweesd dossier'.

7 Uitspraken gedaan in de lezing van Harm Brouwer op het Seminar *RFID en opsporing*, 4 april 2007 in Den Haag, georganiseerd door ECP.nl en het Rathenau Instituut.

8 A.H. Vedder & J.G.L. van der Wees, 'Hoe veilig is de privacy van de doorsnee burger sinds 9/11?', *P&I* 2007, p. 2-8.

9 *PP2CS*, p. 65.

10 *S1VD*, p. 52.

11 *S1VD*, p. 51.

2.4 *Rode draad*

Wij zien een rode draad die deze rapporten met elkaar verbindt.

- Er is telkens sprake van wet- en regelgeving die ruime bevoegdheden biedt. De regels zijn ofwel onduidelijk, ruimhartig, of praktisch non-existent. (De Wet bescherming persoonsgegevens is niet van toepassing op de hier beschreven domeinen.[12])
- Er is vrijwel geen controle op mogelijk misbruik of manipulatie van gegevens door de desbetreffende overheidsdiensten (of ingeschakelde externe partijen).
- Onafhankelijk toezicht is onmogelijk: cijfers die inzicht geven in de mate van gegevensuitwisseling ontbreken; waarborgen voor zorgvuldige omgang met gegevens zijn weinig uitgewerkt; het wettelijke vereiste van betekenisvolle hertelling van stemmen wordt eenvoudigweg niet geïmplementeerd.
- De meeste wet- en regelgeving is zonder noemenswaardig debat of maatschappelijke discussie vastgesteld. De gevoeligheid van de materie wordt bij introductie hiervan niet expliciet aan de orde gesteld.
- Op deze domeinen wordt een gebrek aan visie, sturing en beleid geconstateerd, die de hierboven genoemde punten verklaart.
- Er zijn geen aanwijzingen dat grote ontsporingen zich daadwerkelijk hebben voorgedaan.

In de bovenstaande opsomming is het laatste punt opvallend. Hoe kan het dat er vooralsnog slechts weinig lijkt te zijn misgegaan met de basiswaarden van privacy, veiligheid en democratie, terwijl er zo veel zo slecht geregeld is? De pessimist zal zeggen dat er al heel veel kan zijn misgegaan, maar dat we dat gewoonweg niet hebben waargenomen, juist omdat er zo veel zo slecht geregeld is. De optimist zou kunnen beweren dat bij gebrek aan excessen er geen wijziging in de wet- en regelgeving nodig is.

De vraag blijft hoe het kan dat er niet zo veel mis lijkt te zijn gegaan.

3 Praktische 'garanties'

In het domein van de stemcomputers zijn de problemen uiteindelijk politiek onderkend, met name door de voormalige minister Nicolaï voor Bestuurlijke Vernieuwing en Koninkrijksrelaties, en geanalyseerd in het rapport *S1VD* van de door hem ingestelde commissie Hermans. Er wordt langzaamaan duidelijk dat oplossingen gezocht moeten worden in een juiste combinatie van adequate wet- en regelgeving, open implementatie en betekenisvol toezicht. In de 'oude' situatie is men immers afhankelijk van de zelfbeperking van betrokken partijen om de handelsvrijheid niet te misbruiken en de verkiezingsuitslag niet te manipuleren.

Het gebrek aan garanties in het opsporingsdomein met betrekking tot veiligheid en privacy heeft vooralsnog niet geleid tot een vergelijkbare 'crisis'. In de praktijk lijkt de inbreuk van overheidswege op de privacy van burgers niet zo ver te gaan als het wettelijk kader toestaat. Hiervoor zien wij twee belangrijke verklaringen:

- Het beschavingsniveau en de zelfbeperking van de betrokken partijen (zoals opspoorders).
- Het gebrekkige vermogen van de overheid om effectief met de vergaarde gegevens om te gaan.

Het moge al wel duidelijk zijn dat we het hier niet hebben over harde beschermingsgaranties, gebaseerd op afdwingbare regelgeving.

Het eerste punt hebben we ook al gezien in het domein van de stemcomputers. In het veiligheidsdomein kan dit punt het beste geïllustreerd worden aan de hand van een voorbeeld. Begin maart dit jaar publiceerde *de Volkskrant* een opiniestuk van de huidige auteurs waarin erop gewezen werd dat de populaire Stemwijzer geen privacy policy biedt maar wel politieke voorkeur van de gebruiker (een 'bijzonder' of 'gevoelig' persoonsgegeven) opslaat samen met het gebruikte IP-adres (een 'identificerend' persoonsgegeven).[13] In het opiniestuk werd zijdelings opgemerkt dat onder huidige wetgeving politie en inlichtingendiensten de opgebouwde databank van zo'n 4 miljoen bezoekers gewoon kunnen vorderen in het kader van een onderzoek. Dit ontbreken van een privacy policy heeft enige verdere aandacht getrokken – onder andere omdat het CBP besloot een eigen onderzoek in te stellen – waarbij in de verdere verslaggeving gesuggereerd werd dat de inlichtingendiensten daadwerkelijk geïnteresseerd zouden kunnen zijn in de databank van de Stemwijzer. Hierop reageerde de AIVD, bij monde van de woordvoerder. Er werd nadrukkelijk gesteld dat men zulke databanken niet zal opvragen. Maar er werd toegegeven dat de bevoegdheid om dat te doen wel degelijk bestaat en ook dat men in het verleden wel politieke voorkeur registreerde (met name in communistische hoek). 'Dat was een andere tijd, toen was onze taakomschrijving anders.'[14]

Kortom, bij de ruime wetgeving met betrekking tot gegevensvordering zijn we sterk afhankelijk geworden van het beschavingsniveau en de zelfbeperking van betrokken uitvoerders: van wat zij wel of niet gepast of van deze tijd achten. Het beroep van de hoogste man van het OM op het vertrouwen in het beoordelingsvermogen van zijn organisatie past in deze lijn.

Het tweede punt betreft het onvermogen om effectief om te gaan met de vergaarde gegevens. In *D4D* wordt hier het een en ander over gemeld. Het beschikken over veel gegevens (data) is *an sich* niet bijzonder nuttig, zolang deze gegevens niet in context worden geplaatst, en niet worden gecombineerd met andere gegevens, en niet nader worden geanalyseerd. Doet men dat wél dan ontstaat er *intelligence*, kennis op een hoger niveau die van cruciaal belang is voor besluitvorming, planning, strategieontwikkeling en preventie.[15] Intelli-

12 Art. 2 lid 2 onder b-f WBP.

13 B. Jacobs & W. Teepe, 'Raar dat stemhulp alles van u weet', *de Volkskrant* 6 maart 2007, p. 7.

14 *De Volkskrant* 5 mei 2007.

15 *D4D*, p. 20.

gence staat in Nederland, net als in andere landen, nog te veel in de kinderschoenen.[16] Geautomatiseerde vergaring en uitwisseling van gegevens leent zich voor het toepassen van nieuwe technologieën, zoals datamining, neutrale netwerken en clustering. Dit type technologie kan nuttig zijn bij de omzetting van data in *intelligence*, omdat er grondige analyses mee kunnen worden uitgevoerd die eenvoudigweg niet met de hand te doen zijn. Hierover stelt *D4D*:[17] 'De techniek staat voor het veiligheidsdomein nog steeds in de kinderschoenen en niet iedereen is overtuigd van de waarde daarvan.' En:[18] 'Hier vindt elke partij zijn eigen wiel uit. Betere samenwerking bij het opzetten van systemen voor de nieuwe technologie zal leiden tot veel betere resultaten.'

De samenwerking tussen de partijen in het veiligheidsdomein laat ook op andere gebieden veel te wensen over. Er is een belemmerend gebrek aan visie:[19] 'Door het ontbreken van deze gemeenschappelijke strategische visie op het belang van de gegevensbestanden kunnen de diensten ook niet ten volle effectief gebruik maken van deze bestanden.'

Op een lager niveau, het onderling uitwisselen van vergaarde gegevens, wordt ook te weinig samengewerkt. Dit wordt geweten aan een cultuur waarin vergaarde gegevens als eigendom worden gezien, en uitwisseling met andere diensten daarom veelal niet zonder tegenprestatie gebeurt. Hoewel dit internationaal tussen veiligheidsdiensten gebruikelijk is, wordt in *D4D* gesteld dat dienaren en diensten van dezelfde (nationale) overheid onderling niet op die wijze met elkaar behoren om te gaan.[20]

Bij onderzoeken naar het functioneren van de inlichtingen- en veiligheidsdiensten voorafgaand aan de terroristische aanslagen in New York, Washington, Madrid en Londen zijn veelal vergelijkbare conclusies over het delen en interpreteren van gegevens getrokken: 'Die informatie was dus op zich wel aanwezig, maar was niet altijd op de goede plaats beschikbaar of er waren niet de goede conclusies uit die gegevens getrokken.'[21] Men is er inmiddels wel achter dat daar meer voor nodig is dan simpelweg databanken aan elkaar knopen. De commissie probeert dit naïeve niveau van analyse dan ook te overstijgen, bijvoorbeeld via aanbevelingen voor infobox-achtige samenwerking en *fusion centers* voor gezamenlijke interpretatie van gegevens.[22] In dit verband is het opvallend dat er in *D4D* met geen woord gerept wordt over onze eigen terroristische polderaanslag, de moord op Theo van Gogh, en met name over de daar aan voorafgaande vergaring, deling en interpretatie van gegevens. Deze kwestie is nog in onderzoek bij de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Misschien leren we daarvan te zijner tijd meer.

De diensten in het veiligheidsdomein halen bepaald niet het onderste uit de kan, zoveel is duidelijk. Met het verschijnen van *D4D* is daarover in Nederland geen discussie meer mogelijk. Voor de bescherming tegen terroristische aanslagen is dit een zorgelijke constatering, maar voor de privacy van de burger is de duiding ambivalent. Enerzijds kan men veronderstellen dat als het niet altijd lukt de verzamelde puzzelstukjes van vermeende terroristen bij elkaar te leggen, dit bij de puzzelstukjes van de brave burgers ook wel niet zal lukken. Anderzijds is het natuurlijk merkwaardig dat er zo veel puzzelstukjes verzameld worden zonder dat deze uiteindelijk effectief benut worden.

Het onvermogen van de overheid om effectief met de vergaarde gegevens om te gaan kan gezien worden als een praktische garantie voor de privacy van de brave burger. Zo'n onvermogen is natuurlijk een armoedig soort garantie en een wankele basis voor vertrouwen. Je geeft immers ook je bankpas met bijbehorende pincode niet weg, zelfs als je weet dat de ontvanger er niet mee om kan gaan.

Deze praktische garanties voor de privacy van de burger kunnen als volgt omschreven worden. Opspoorders hebben het *vermogen* om te kiezen voor 'gepast' gebruik van hun informationele bevoegdheden, en hebben het *onvermogen* om de vergaarde gegevens voldoende effectief te analyseren. De auteurs van *PP2CS* stellen 'Als de overheid zich als Big Brother wil gaan gedragen, zijn de wet en de techniek er klaar voor.'[23] De overheid is daar zelf kennelijk nog niet klaar voor.

4 Draagvlak voor daadkracht

De gebrekkige garanties voor betrouwbare verkiezingen, zoals beschreven in *S1VD* hebben in 2006 tot een maatschappelijk debat geleid. De stichting <wijvertrouwenstemcomputersniet.nl>maakte bezwaar tegen met name het *black box* karakter van de eerste generatie stemcomputers, waarbij de burger geen garantie heeft dat de uitgebrachte stem ook daadwerkelijk (ongeschonden) bijdraagt aan het eindresultaat. Door technisch onderlegde betogen, geslaagde demonstraties, effectieve mediaoptredens en gerichte bestuurlijke en juridische acties heeft deze stichting de eigen zorgen tot een nationale kwestie weten te maken, waarbij de goedkeuring van een van de twee gebruikte types stemcomputers door de verantwoordelijke minister ingetrokken is. Het rapport *S1VD* is een direct gevolg van deze campagne. Het rapport heeft de stichting op zo ongeveer alle punten gelijk gegeven. De commissie constateert onder andere dat de overheid nalatig geweest is, niet adequaat op signalen gereageerd heeft, te veel heeft overgelaten aan ingewijden (normen voor stemcomputers werden bijvoorbeeld geschreven en gecontroleerd door een en dezelfde instantie) en van burgers werd verwacht simpelweg vertrouwen te hebben in een oncontroleerbare gang van zaken.

Zijn er parallellen met het veiligheidsdomein? Het gaat in beide gevallen over het (gebrekkige) gebruik van IT door de overheid in de omgang met basiswaarden als privacy, veiligheid en democratie. Is dan ook op veiligheidsgebied een opstand van burgers te verwachten tegen gevraagd vertrou-

16 Conclusie 2, *D4D*, p. 10.
17 *D4D*, p. 49.
18 *D4D*, p. 99.
19 *D4D*, p. 98.
20 *D4D*, p. 98-99.
21 *D4D*, p. 18.
22 *D4D*, p. 109-111.
23 A. Vedder, L. van der Wees & E.J. Koops, 'Big Brother's bevoegdheden zijn er – nu hij zelf nog?', *NJB* 2006/41, p. 2356-2360.

wen zonder fundament? Zijn er nieuwe stichtingen op komst met voorspelbare namen als: wijvertrouwendataretentieniet.nl, wijvertrouwencentraleopslagbiometrieniet.nl en wijvertrouwendataminingniet.nl, of zelfs wijvertrouwendeaivdniet.nl en wijvertrouwendeoverheidniet.nl. Is het verstandig te blijven rekenen op kritiekloze instemming van burgers met maatregelen waarbij de burgers geen controle hebben over en inzicht hebben in het gebruik van hun gegevens, waarbij de overheid geen oog heeft voor proportionaliteit en subsidiariteit (*D4D*) en waarbij uiteindelijk de machtsbalans tussen overheid en burgers in het geding is? Het is mogelijk dat de ontwikkelingen rond stemcomputers verdergaande invloed hebben en tot meer recalcitrantie leiden.

Met name hier wreekt zich het grote punt uit *D4D* dat een gemeenschappelijk en gedragen visie op gegevensbevraging en gegevensverwerking door de opsporingsdiensten ontbreekt. Zo'n visie is noodzakelijk voor blijvend draagvlak.

In het rapport *D4D* wordt zo'n visie niet ontwikkeld. Daarvoor is volgens *D4D* een vervolgstudie nodig. Aanzetten tot zo'n visie zouden gevonden kunnen worden in het selectief en volgens heldere regels omgaan met de beschikbare bevoegdheden (*select before you collect*,[24] in plaats van andersom), in het uitwerken van *revocable privacy* voor overtreders, en in het ontwikkelen van toezicht op en verantwoording door opspoorders (niet slechts een controlestaat maar ook een controle-controlestaat).

Het rapport *D4D* draagt ruim stof aan voor discussie. Met betrekking tot stemmen heeft het decennialang ontbroken aan visie en adequate regelgeving. Ondanks het ontbreken van daadwerkelijke ontsporingen heeft dit uiteindelijk geresulteerd in het wegvallen van draagvlak. Met betrekking tot de strijd tegen terrorisme en criminaliteit wijzen wij hier op de mogelijkheid van een vergelijkbaar scenario.

Dat is het scenario waarin het *vermogen* tot vrijwillige en 'gepaste' zelfbeperking van diensten in het veiligheidsdomein ter discussie staat. En ook het scenario waarin het *onvermogen* om de vergaarde gegevens tot het uiterste te analyseren wel eens zou kunnen verdwijnen. Bij zulk afnemend onvermogen wordt mogelijk een te groot beroep gedaan op dit vermogen, en is regulering daarvan wenselijk.

24 B. Jacobs, 'Select before you collect', *AA* 2005, p. 1006-1009.