

Variaties op een thema: van paspoort- naar identiteitsfraude

Een gokje. Over vijf jaar staat het volgende bericht op de voorpagina van diverse landelijke dagbladen: 'Lichaamskenmerken van vele miljoenen burgers op straat. Bij een 'hack' bleken beveiligingsexperts in staat zich zonder al te veel moeite toegang te kunnen verschaffen tot de landelijke databank waarin biometrische gegevens van ons gezicht en onze vingers zijn opgeslagen.'

Corien Prins is hoogleraar recht en informatisering aan de Universiteit van Tilburg en redacteur van dit blad.

Een onrealistisch scenario? Verre van. In feite vond namelijk een soortgelijk voorval afgelopen september al plaats. Toen bleken ruim 1,2 miljoen patiëntgegevens na een computerkraak van enkele ziekenhuissystemen vrij toegankelijk voor hackers. Voor techneuten was het wellicht niets meer dan een vingeroefening voor een toekomstige kraak van de landelijke of Europese biometrie-databank. In politiek Den Haag werden naar aanleiding van de kwestie met de patiëntgegevens direct de nodige kamervragen gesteld, beloofde de verantwoordelijk minister beterschap en staat de beveiliging van databanken en computersystemen in de 'zorgketen' inmiddels hoog op de ambtelijke agenda. De invoering van het elektronisch patiëntendossier is er zelfs een jaar voor uitgesteld. Een goedbedoelde blijk van beterschap. Meer dan dat is het, zo vrees ik, niet. De tweederangs aandacht voor de kwetsbare kanten van computersystemen, databanken en elektronische identificatiesystemen lijkt namelijk een structureel probleem bij onze (semi-)overheid. En dan heb ik het niet alleen over de organisaties die in de dagelijkse praktijk verantwoordelijk zijn voor de beveiliging van computersystemen, maar zeker ook over zowel de relevante politiek beslissingen als de daarmee samenhangende wetgeving.

Het gaat niet alleen techneuten aan

Voer voor techneuten, zo hoor ik u zeggen. Maar er is meer aan de hand en er zijn goede redenen om de kwestie van beveiliging, gegevensbestanden en identificatiesystemen juist vanuit wetgeving en achterliggende beleidsoverwegingen te benaderen. Even kort voor wie er nog niet bij had stilgestaan: mede onder druk van de Verenigde Staten werken Nederland en de overige lidstaten van de Europese Unie al enige tijd aan de invoering van biometrie op het reisdocument. Kort gezegd wordt bij biometrie gebruik gemaakt van een digitale afdruk van lichaamskenmerken, zoals vingerafdruk, iris of gezicht. Aan de hand van deze kenmerken kan een unieke identificatie van de bij het reisdocument behorende persoon worden gerealiseerd, zo is de stelling. Wederom een stap in de strijd tegen paspoortfraude. En wat gebeurt er met de informatie over de gebruikte lichaamskenmerken? 'In het kader van terrorismebestrijding' acht de politiek het noodzakelijk dat deze in een centrale databank worden opgeslagen. Bovendien is de ambitie uiteindelijk niet beperkt tot een nationale databank, maar komen de gegevens over gezicht, iris of vinger van alle Europese burgers op EU-niveau beschikbaar. November 2005 publiceerde de Europese Commissie een document met plannen voor een Europees vingerafdrukkenregister dat automatisch doorzocht kan worden. Elke reiziger zal in de lidstaten zowel bij binnenkomst als bij vertrek worden geregistreerd met behulp van biometrische gegevens. Opsporings- en inlichtingendiensten krijgen vervolgens ruim toegang tot al deze gegevens. Bovendien wil de Europese Commissie dat de nationale DNA-databanken met de vingerafdrukkenregisters worden verbonden tot zogenaamde 'super-registers'. Nieuw daarbij is ook het uitgangspunt dat een buitenlands informatieverzoek op dezelfde wijze als een binnenlands informatieverzoek zal worden behandeld. De vraag of een buitenlandse dienst wel een legitieme reden heeft om de informatie op te vragen, of het om feiten gaat die in Nederland ook strafbaar zijn, dan wel of er voldoende garanties zijn dat verdachten een fatsoenlijke rechtsgang tegemoet kunnen zien, zijn in de plannen van de Commissie niet langer relevant bij de toetsing voor toegang tot de biometrische gegevens. Onderliggend idee is dat de

rechtsstelsels van de Europese lidstaten weliswaar sterk van elkaar verschillen, maar gelijkwaardig zijn, aldus de Europese Commissie.

En het gaat om veel meer dan privacy

Vergaande maatregelen. Maar nauwelijks discussie. Opvallend genoeg lijkt bovendien niemand er bij stil te staan dat uit opgeslagen lichaamskenmerken mogelijk ook geheel andere kennis is af te leiden. Zo heeft onderzoek bij Philips naar 'oorbiometrie' laten zien dat aan de hand van de digitale afdruk van het oor (opgeslagen op een zogenaamde template) de Russische subjecten in een databank zijn aan te wijzen. Bekend is dat Aziatische vingerafdrukken minder diep zijn dan die van westerse personen en ook dit kan consequenties hebben voor de informatie die uit een template is af te leiden. Kortom, het is heel wel mogelijk dat - afhankelijk van het type template - in de toekomst kenmerken als ras en geslacht uit de opgeslagen informatie is af te leiden. Je zou kunnen stellen dat de politiek dus via een achterdeur stillertjes een in potentie zeker zo waardevolle pendant als de - wel flink bediscussieerde - algemene databank met DNA-gegevens realiseert. Bovendien opteert men voor het gebruik van onder meer gezichtsherkenning. De beleidsverantwoordelijken hebben daarmee impliciet ook gekozen voor een identificatietoepassing die zonder dat de betreffende persoon zelf zich dat behoeft te realiseren toegepast kan worden. Tenslotte, biometrie wordt in Den Haag en Brussel gepresenteerd als de ultiem betrouwbare vorm van identificatie. Zo veilig is ons paspoort nog nooit geweest, zo lijken beleidsmakers te roepen. Recente studies in het Verenigd Koninkrijk laten ons echter zien dat het foutpercentage voor biometrie met behulp van gelaatsherkenning 31% is. Een test in de Verenigde Staten met gezichtsherkenning liet een foutpercentage van 53% zien. Verontrustend hoge getallen. Daarbij moet ook nog eens worden bedacht dat het een testpopulatie zonder fraudeurs betrof. Ik zou zeggen: waar blijft het debat?

Niemand zal ontkennen dat een betrouwbare identificatie of verificatie van burgers een punt van aandacht moet zijn en dat technologie een belangrijke rol speelt bij identificatieprocessen. En natuurlijk zie ook ik dat het niet eenvoudig is om de complexe dynamiek van het gebruik van techniek ten behoeve van de uitvoering van beleid te duiden. Mijn stelling is echter dat de politiek de kop in het zand steekt voor de verre gaande implicaties en de kwetsbare kanten van de keuzes die momenteel worden gemaakt. Te vaak beroepen politici zich op eenvoudig te formuleren belangen als veiligheid en fraudebestrijding. In essentie gaat het echter niet om deze en andere min of meer praktische belangen, maar om de fundamentele kwestie hoe wij de ordening van onze informatiesamenleving vorm willen geven, hoe de positie van burgers daarin te zien en hoe kwetsbaar wij ons als techniekafhankelijke maatschappij willen opstellen. Daarover dient het debat in onze volksvertegenwoordiging te gaan. Niet zozeer over zaken als '(vermindering van) het aantal fouten bij invoering en verwerking van persoonsgegevens, (...) een meer klantgerichte dienstverlening, een betere bescherming tegen identiteitsfraude en het vergroten van transparantie van de overheid', om vier veelgehoorde en centrale beleidsargumenten te citeren. Al deze argumenten zijn namelijk stuk voor stuk voor discussie vatbaar. Wie wil weten waarom, moet een geheel ander identificatie-initiatief maar eens kritisch doornemen: het Burgerservicenummer (BSN). Een nieuw, algemeen en uniek persoonsnummer dat oorspronkelijk afgelopen 1 januari, maar nu later dit jaar, ons sofi-nummer moet vervangen. De drie argumenten rondom het BSN op een rij.

Argument 1: vermindering van het aantal fouten

Fouten moeten worden voorkomen en de doelmatigheid van de overheidsadministraties valt aanzienlijk te verbeteren. Zeker. Anders dan de voorstanders van het BSN echter ben ik van mening dat deze ambities niet samenvallen met de noodzaak tot de introductie van een algemeen en breed koppelbaar identiteitsnummer. Wellicht zal de introductie van het BSN het *aantal* fouten verminderen. Gegevens hoeven immers niet langer iedere keer ingevoerd te worden, waardoor de kans op missers afneemt. Maar met een discussie over aantallen fouten zijn we er niet. Tien fouten in los van elkaar functionerende systemen kan heel wat minder ellende met zich meebrengen dan één zich snel verspreidende fout in een centraal systeem waarbij niemand meer het gevoel heeft dat het zijn of haar fout is. En wat is het effect van de schijnbaar autonome dynamiek wanneer een onjuist persoonsgegeven verzeild raakt in het

welhaast oneindig gekoppelde informatiesysteem van onze overheid? Bij welk - anonieme - loket moet de burger aankloppen om de fout te herstellen? Welke procedures moet hij doorlopen alvorens de fout is vastgesteld en erkend? En hoe lang moet hij wachten voordat de correctie vervolgens in alle aangehaakte systemen is doorgevoerd? Het zijn vragen die tot nu toe onbeantwoord zijn gebleven. Laat staan dat er voldoende aandacht is besteed aan heel praktische vragen als de beveiliging van systemen en bestanden die gebruik maken van het BSN. Aan structurele, in de wet verankerde, aandacht en garanties voor opschoonplichten, controle, audits en andere corrigerende maatregelen ontbreekt het helaas in het overheidsinformatiebeleid. Dat geldt helaas ook voor het wetsvoorstel BSN. Het rept met geen woord over deze kwesties. Juist de gebrekkige kwaliteit van veel achterliggende gegevensbestanden heeft belangrijke consequenties voor de uitvoering van overheidstaken, het imago van de overheid, het wederzijdse vertrouwen van samenwerkende instanties, het instandhouden van schaduwregistraties (zo houdt de politie er een schaduwregistratie op na omdat ze niet op de GBA kan vertrouwen), etc. De vraag of de invoering van een centraal en uniek nummer een bijdrage levert aan, of op z'n minst een prikkel geeft tot, een kwaliteitsverbetering van alle achterliggende gegevens en systemen, is hoogst twijfelachtig. En juist in het licht van de hierna aan te kaarten risico's voor de burger, is daarmee de vraag naar de noodzaak van initiatieven als het BSN (maar zeker ook biometrie) niet beantwoord. Veel fundamenteeler echter en daarmee ook breder dan de BSN-discussie, is het volgende: beleidsmakers lijken een absoluut vertrouwen in techniek en systemen te hebben en daarmee ook het gevoel te bezitten dat het perfect opgetuigde identificatie- en controlesysteem geen fouten meer toelaat. We zien dit onterechte vertrouwen bij biometrie en we zien het bij het BSN. En daarmee vormt het een risico op zichzelf. Opdracht 1 voor de overheid is derhalve het uitzetten van gedegen onderzoek naar de kwetsbare kanten (zeker ook de op termijn kwetsbare kanten) en dus de nadelen van identificatie-instrumenten als biometrie en BSN. Pas als deze inzichten op tafel liggen en worden afgewogen tegen de voordelen, kan sprake zijn van een verantwoorde beleidskeuze. Nu is dat zeker niet het geval.

Argument 2: meer klantgerichte dienstverlening

Klantgerichte dienstverlening is de kreet die via vele symposia, beleidsdocumenten en andere kanalen tot ons komt. De overheid ziet ons niet langer als een van die miljoenen anonieme burgers die gebruik maken van talloze overheidsdiensten. Nee, we mogen ons er waarlijk over verheugen tot de klantenkring van de overheid te behoren. In werkelijkheid zijn we bij deze aanbieder natuurlijk een heel ander soort klant dan op de markt van private diensten en producten. Overstappen naar een concurrent als we niet tevreden zijn, blijkt lastig. Invloed uitoefenen op het aanbod aan diensten en producten is er bij deze dienstverlener niet bij. Nee, 'klantgerichte' dienstverlening bij de overheid is niets anders dan inzetten op efficiëntere processen, geïnitieerd en gestuurd vanuit de overheid met aan overheidszijde gedetailleerde kennis over de zaken waar de burger zoal recht op heeft (of juist geen recht op heeft). De werkelijke belanghebbenden bij het BSN zijn zeker niet de burgers. Illustratief in dit opzicht is de kritiek van de Raad van State op het wetsvoorstel BSN. Het verbaast de Raad dat het voorstel alleen over de burger spreekt als een object. En hij fronst de wenkbrauwen over de keuze voor de benaming 'burgerservicenummer'. Een aanduiding als 'algemeen registratienummer' of iets dergelijks had naar het oordeel van de Raad meer voor de hand gelegen. Wie de ontwikkelingen bij de overheid goed volgt, stelt vast dat onder het motto van klantgerichte dienstverlening de rollen in feite worden omgedraaid. In toenemende mate haalt de overheid het initiatief naar zich toe en wordt bezien of u al dan niet recht heeft op een bepaald overheidsinitiatief (vgl. de campagne rondom de zorgtoeslag: 'u hoeft zelf niets te doen') Het zijn lokale overheden die inwoners erop attenderen dat ze vergeten zijn gebruik te maken van hun recht op huursubsidie. Het is de belastingdienst die volautomatisch voor ons een verzoek om voorlopige teruggave van belasting opstelt. Een alwetende overheid die met behulp van nieuwe technieken voor profilering haar burgers een bepaald 'klant-profiel' - een nieuw soort 'identiteit' - opplakt en aan de hand daarvan precies weet welke rechten en plichten wij hebben. Een overheid die ons naar eigen inzicht diensten aanbiedt dan wel (buiten ons weten om) juist daarvan uitsluit. Het resultaat: een afgedwongen ommezwaai in de traditionele rolverdeling tussen burger en publieke sector. Eigen initiatief van burgers wordt losgelaten, met

als mogelijk gevolg: afkalven van de individuele vrijheid van burgers om zich naar de overheid toe op een bepaalde manier en in een bepaalde hoedanigheid te profileren. Dwars doen, stout zijn of gewoon simpel iets vergeten of je vergissen is er niet meer bij. De overheid weet alles en beslist volautomatisch over alles en iedereen. En u raadt het al: juist het BSN speelt in dit scenario een voorname rol. En met de informatie die op termijn uit biometrische gegevens is af te leiden, zal de overheid over nog meer nuttige informatie beschikken.

Als opdracht 2 zou ik de overheid willen uitdagen waarlijk openheid van zaken te geven over specifieke beleidsmotieven, gebruikte gegevensbestanden, toegepaste profielen en ingezette technieken die een rol spelen bij het beleid om individuele burgers in of uit te kunnen sluiten van bepaalde diensten dan wel hen op maat object van overheidsbeleid te doen zijn.

Argument 3: betere bescherming tegen identiteitsfraude

De aanpak van identiteitsfraude is, naar ik vrees, de belangrijkste reden waarom de overheid inzet op de introductie van het BSN, biometrie en andere op technologie en centrale databanken gestoelde toepassingen voor identificatie. Er zijn echter gegronde redenen om te twifelen aan de effectiviteit van deze initiatieven in de strijd tegen deze snel aan populariteit winnende vorm van criminaliteit. Het zou zelfs, zoals ik in een publicatie van ruim twee jaar geleden al opmerkte, heel wel op een tegenovergestelde ontwikkeling kunnen uitlopen: de huidige plannen rondom identificatie dragen juist bij aan de verdere opmars van identiteitsfraude. Ook het College Bescherming Persoonsgegevens wees afgelopen najaar op dit risico: 'Identiteitsfraude zal toenemen. Dit mag zonder meer verwacht worden op grond van Nederlandse en buitenlandse ervaringen. Ook nu wordt er illegaal gebruik gemaakt van het sofi-nummer van anderen, hetgeen voor de rechtmatige houder van het sofi-nummer hoogst onaangename gevolgen kan hebben, evenals voor de mogelijk daarbij betrokken werkgevers, verzekeringsmaatschappijen en overheidsinstanties. Door de veel bredere toepassing van het BSN zal deze vorm van identiteitsdiefstal aanzienlijk lucratiever worden en dus vaker voorkomen en grotere gevolgen hebben. Het wetsvoorstel gaat aan dit probleem voorbij.' In feite kunnen we stellen dat de overheid niets heeft geleerd van de eerdere problemen met het sofi-nummer. Ze trekt zich kennelijk ook niets aan van ervaringen in andere landen met identiteitsfraude dan wel waarschuwingen van deskundigen. Vanuit de ijdele hoop dat met een herhaling van argumenten wellicht toch wat bij de verantwoordelijk politici beklijft, zet ik de kwetsbare kanten nog maar eens op een rij. Het sofi-nummer heeft zich de laatste jaren een ruime toepassing en daarmee ook brede verspreiding eigen gemaakt. Het nummer staat inmiddels niet alleen in ons paspoort, maar wordt (al dan niet terecht) door een scala aan publieke en private instanties opgevraagd en vervolgens opgeslagen. Juist vanwege deze brede verspreiding en het gemak waarmee het in de vele - in toenemende mate gekoppelde - informatiesystemen wordt rondgepompt, is het nummer zo kwetsbaar voor fraude gebleken. Verandert deze situatie met de invoering van het BSN? Het ziet ernaar uit van niet. Spijtig genoeg merkt de Memorie van Toelichting nogal makkelijk op dat aan mogelijk gebruik door het bedrijfsleven bewust geen aandacht is geschonken. 'De problematiek met betrekking tot het gebruik van persoonsnummers door het bedrijfsleven, is namelijk van andere aard dan de introductie van een algemeen persoonsnummer voor de overheid.' Om er vervolgens eufemistisch aan toe te voegen: 'Het wetsvoorstel werpt overigens geen nieuwe belemmeringen op voor het gebruik van persoonsnummers door bijvoorbeeld het bedrijfsleven.' Het zal niet verbazen dat VNO/NCW zich al een warm voorstander van gebruik door de private sector heeft getoond. En Minister Zalm maakte afgelopen november tijdens een debat met de Tweede Kamer bekend de banken via het BSN toegang te willen verlenen tot de gemeentelijke administratie. Bankieren kunnen aldus gegevens zoals naam, adres en woonplaats uit de bevolkingsadministraties ophalen. Maar dat lijkt een wat simpele weergave van de informatie die de private sector uiteindelijk in handen krijgt. Kenmerkend voor het BSN is nu juist dat het een centraal en uniek nummer wordt. Kortom, toegang tot het BSN betekent voor de private sector ook toegang tot ons onderwijsnummer, zorgnummer, huursubsidienummer, etc. Voor de Raad van State is het duidelijk waar het uiteindelijk allemaal toe zal leiden: 'Het BSN is in principe openbaar: het zal worden vermeld op identiteitsbewijzen; bedrijven kunnen het BSN langs die weg dan ook registreren en gebruiken. (...) het zal in de praktijk niet zijn tegen te houden dat het BSN van diverse personen ruim bekend wordt, en soms zelfs op internet

opduikt (...) door het combineren van de gegevens die dat oplevert ('data-mining') kan dan een indringend beeld van zo'n persoon worden opgebouwd.'

Ervaringen in het buitenland laten zien dat met iedere stap in de richting van een integratie van systemen, onze samenleving tegelijkertijd ook afhankelijker wordt van het adequaat functioneren van dat ene centrale systeem en zich daarmee juist kwetsbaarder maakt voor identiteitsfraude. En breed gebruik door de private sector verergert de situatie alleen maar. Want zodra instrumenten zoals het BSN en biometrie belangrijke maatschappelijk en juridische instrumenten voor identificatie blijken, is het per definitie een gewild object voor fraudeurs. Daarbij versterkt de vermeende hogere kwaliteit van deze nieuwe instrumenten ook nog eens het vertrouwen in de geclaimde valse identiteit. Identiteitsfraude staat in de Verenigde Staten en diverse ons omringende landen hoog op de politieke agenda. Daar zijn al vele tientallen miljoenen burgers het slachtoffer van deze snel aan populariteit winnende vorm van criminaliteit. Maar het lijkt alsof de overheid vanuit een soort van technocratische vervreemding dit probleem niet wenst te onderkennen. Het wetsvoorstel BSN rept, ondanks het expliciete verzoek daartoe van de Raad van State, met geen woord over een mogelijk neveneffect als identiteitsfraude. We weten in feite ook nog nauwelijks iets van de risico's die we in ons land lopen met identiteitsfraude. Wat maakt de specifieke wijze waarop we in ons land de identificatie-infrastructuur hebben ingericht nu kwetsbaar voor identiteitsfraude? Valt een indicatie te geven van de mogelijke omvang en maatschappelijke consequenties van het probleem? Evenmin beschikken we over inzicht in de mate waarin maatschappelijke factoren bij identiteitsfraude een rol spelen. Het kan immers heel wel zijn dat de sociale context een rol speelt bij identiteitsfraude (bepaalde sociale klassen of bevolkingsgroepen zijn mogelijk kwetsbaarder voor identiteitsfraude en hebben vervolgens aanzienlijk meer moeite fraude aan te tonen dan wel hun identiteit weer op de rails te krijgen). En wat, ten slotte, te doen met een ontwikkeling als *privacy flooding*? Het credo van deze vlucht vooruit: maak uw gevoelige gegevens bewust openbaar zodat ze daarmee hun zin verliezen. Met andere woorden, zet informatie over uw vingerafdruk bewust op het internet, beweer dat iemand anders deze informatie van het web heeft gehaald en in siliconen heeft nagemaakt en biometrische identificatie is daarmee zinloos geworden. Het zijn de bovenstaande en vele andere fundamentele vragen die spijtig genoeg in het huidige debat over identificatie en identificatie-instrumenten onbeantwoord blijven.

Oprichting 3, ten slotte, is het initiëren van onderzoek naar de risico's van identiteitsfraude in Nederland. Daarbij moet aandacht zijn voor de specifieke context waarin identificatie in ons land vorm heeft gekregen dan wel zal krijgen. De implicaties van gebruik door de private sector zullen kritisch bekeken moeten worden. En tenslotte zal er ook gereflecteerd moeten worden op de gegevens en onderzoeken over identiteitsfraude die inmiddels in andere landen beschikbaar zijn gekomen. Kortom, overheid: analyseer onze eigen situatie met oog voor de lessen uit het buitenland. En gebruik de uitkomsten vervolgens ook daadwerkelijk bij de beleidskeuzes op dossiers als BSN en biometrie.

Kwetsbaar door vele verborgen gebreken

Afsluitend en concluderend: het huis van onze nationale identificatie-infrastructuur wordt vanuit een welhaast onwrikbaar vertrouwen in de nieuwe technologische mogelijkheden grondig verbouwd. De architect van het nieuwe bouwwerk lijkt echter vanuit zijn geloof in de prestaties van techniek en systemen nauwelijks oog te hebben voor de omgeving waarin het bouwwerk komt te staan. Waarnemingen op het intermenselijk niveau kunnen de bouwtekening kennelijk niet beïnvloeden. Implicaties voor het fundament waarop het huis is gebouwd worden niet onderzocht dan wel halsstarrig genegeerd. Het resultaat is een constructie met vele verborgen gebreken, neergezet op een onvoldoende uitgebalanceerde ondergrond. Maar weldra komen de eerste scheurtjes aan het licht. En denk vooral niet dat het debat dan nog een ogenschijnlijk puur academische exercitie is: de hack van de Europese biometrie-databank is dichterbij dan u wellicht mocht denken.