Identiteitsfraude en overheid

J.H.A.M. Grijpink*

Wereldwijd en in landen met zeer uiteenlopende rechtsculturen worden identiteitscontroles verscherpt ter vergroting van de veiligheid. De overheid wil in steeds meer situaties met meer betrouwbaarheid kunnen vaststellen ófwel *wie* iemand is ófwel of iemand de *juiste* persoon is (hiervoor hoeft men niet te weten wie iemand precies is). Dit wordt belangrijker naarmate in de toekomst meer transacties elektronisch en op afstand plaatsvinden, zonder de sociale controle en het oogtoezicht waarop een traditionele samenleving is gebaseerd.
Ook identiteitscontroles zullen steeds vaker elektronisch en op afstand plaatsvinden. Daarom zullen we voor persoonsherkenning en identiteitscontroles in de toekomst over een breed arsenaal aan identiteitsinstrumenten moeten kunnen beschikken. Naast elektronisch leesbare identiteitsbewijzen, pasnummers, persoonsnummers, pincodes en wachtwoorden, zal bijvoorbeeld ook biometrie noodzakelijk zijn. Met biometrie wordt bedoeld dat men kenmerken van het lichaam (bijvoorbeeld de vingerafdruk of de stem) gebruikt om iemand elektronisch te herkennen. Administratieve gegevens, zoals een persoonsnummer, hebben geen directe relatie met een persoon, waardoor ze voor het doel van identiteitscontrole niet dezelfde waarde hebben als een biometrisch kenmerk.

Identiteitsfraude en identiteitsdiefstal

We moeten het voorlopig nog doen met twee ongelukkige vertrekpunten. In de eerste plaats is het beheer van identiteiten als overheidstaak territoirgebonden. Dat betekent dat identiteitscontrole in het buitenland door de desbetreffende buitenlandse overheid

* Prof. dr. mr. Jan Grijpink is als raadadviseur werkzaam bij de directie algemene justitiële strategie van het ministerie van Justitie, met informatiestrategie als zijn speciale aandachtsgebied. Hij is als bijzonder hoogleraar verbonden aan het Departement informatica en informatiekunde van de Universiteit Utrecht met als leeropdracht *Keteninformatisering in de rechtstaat*.

wordt gedaan volgens de eigen regels en met het oog op de eigen belangen. Dat staat op gespannen voet met de ontwikkeling van de elektronische communicatie, die de gehele wereld omspant en extra dimensies krijgt door toenemende mobiliteit en anonimisering. Een overheid kan zodoende haar onderdanen steeds minder effectief beschermen tegen misbruik van hun nationaal geborgde identiteit.
In de tweede plaats richt het huidige identiteitsbeleid zich, althans in de westerse wereld, op bestrijding van valse en vervalste identiteitsbewijzen en bestaat een identiteitscontrole doorgaans uit controle van het identiteitsbewijs. Maar frauduleus gebruik van een *geldig* identiteitsbewijs van iemand anders (zogenaamde lookalike fraude) drukt ons steeds vaker met de neus op het meer indringende probleem van identiteitsfraude of identiteitsdiefstal. Daarmee bedoelen we dat iemand met opzet de schijn oproept van een identiteit die niet bij hem hoort. Een identiteitsbewijs is daar niet per se voor nodig. Ook persoonsnummers, foto's, handelingen of gebeurtenissen bevatten allerlei identiteitssuggesties waaruit mensen een conclusie trekken over wie ze tegenover zich hebben. Identiteitsfraude kan daarom overal en op velerlei manier plaatsvinden en is niet beperkt tot specifieke situaties, procedures of documenten. Nadat de persoonsverwisseling ergens is gelukt, kan de verzonnen of gestolen identiteit vervolgens in allerlei andere situaties volgens daar geldende regels worden gebruikt. Daar kan men de frauduleuze persoonsverwisseling vaak niet meer doorzien.
Onze focus moet daarom niet langer vooral het identiteitsbewijs zijn, maar eerder de persoon die er zich van bedient. Niet de kwaliteit van een identiteitsdocument maar de kwaliteit van het proces van identiteitscontrole zelf vormt steeds vaker de doorslaggevende factor. En identiteitscontrole zal zich in de toekomst steeds vaker buiten de landsgrenzen moeten bewegen, omdat buitenlandse overheden niet zelf over voldoende middelen en gegevens beschikken om misbruik van identiteiten uit andere landen te voorkomen.
De opbouw van het artikel is als volgt. Eerst laten we zien dat identiteitsfraude door de voortschrijdende digitalisering van de samenleving een steeds grotere impact krijgt en dat bestrijding ervan bemoeilijkt wordt door de huidige handhavingspraktijk. Zelfs in de strafrechtketen vindt identiteitsfraude plaats op een schaal die de effectiviteit van de strafrechthandhaving in gevaar brengt. Dat belooft weinig goeds voor andere ketens en sectoren die over minder rechtsmiddelen beschikken. Vervolgens bezien we hoe aan

het groeiende probleem van identiteitsfraude het hoofd kan worden geboden. Wij zullen verduidelijken dat de bij de huidige werkwijzen bestaande en nieuwe instrumenten een groot risico in zich bergen dat deze het probleem eerder vergroten dan verkleinen. Enkele oplossingsrichtingen worden aangegeven voor effectievere werkwijzen. Aan de orde komen ook enige actuele vragen rond privacy en veiligheid bij gebruik van biometrie en bij identiteitscontrole met gegevens die niet op het identiteitsbewijs staan. We besluiten met conclusies en aanbevelingen.

Nieuw identiteits- en identiteitscontrolebeleid nodig

Is identiteitsfraude in de hierboven aangeduide ruime betekenis iets nieuws voor de overheid? Nee, maar de voortschrijdende digitalisering in een mobieler en anoniemer wordende samenleving geeft identiteitsfraude en identiteitsdiefstal wel nieuwe dimensies die de impact vergroten en de bestrijding frustreren.

Méér sporen, minder bewijs

In een digitale omgeving laat ons handelen weliswaar steeds meer sporen achter, maar bij verdenking van een strafbaar feit worden die sporen door de politie spontaan voor sporen van de dader gehouden. Iemands internetadres kan echter evengoed door iemand anders (lijken te) worden gebruikt, dat kun je aan het spoor zelf niet zien. Bij een geslaagd meeliften op de identiteit van iemand anders leiden sporen altijd naar het slachtoffer, niet naar de dader. Het slachtoffer moet dan bewijzen dat hij iets niet heeft gedaan. Dat lukt vaak niet, zodat ondanks alle protesten overheidsinstanties blijven geloven dat de aangetroffen sporen dadersporen zijn, zelfs als zij dat eigenlijk evenmin kunnen bewijzen. Als identiteitsfraude in de toekomst blijft toenemen, zal opsporingsonderzoek bij gebrek aan bewijs steeds vaker vastlopen of vaker leiden tot bestraffing van onschuldigen. Eigenlijk kunnen alleen preventieve maatregelen uitkomst brengen, maar die werken bij de huidige bestuurlijke aanpak vanuit overheid vaak averechts, zoals we hieronder zullen zien.

Olievlekwerking van identiteitsfraude

Geslaagde identiteitsfraude op een zwakke plek ergens in een bepaalde keten verspreidt zich ongemerkt naar andere ketens en processen. Als men op iemands rijbewijs kan meeliften bij het aangaan van een nieuwe arbeidsverhouding, vindt belastingheffing bij het slachtoffer plaats; bij het te naam stellen van een kenteken kan men heffingen, boetes en incasso's ontlopen. In de zorg kan men zo medische behandeling krijgen, ook als men daar geen recht op heeft. En de gegevens worden opgeborgen in het medische dossier van de houder van het rijbewijs. Identiteitsfraude verspreidt zich als een olievlek tot in de kleinste administratieve haarvaten van allerlei maatschappelijke processen waar men de geslaagde primaire identiteitsfraude vaak niet meer kan doorzien.

Machtsverschuiving in een gedigitaliseerde omgeving

Een derde nieuw kenmerk hangt samen met een verschuiving in de machtsverhouding bij identiteitscontroles tussen controleur en gecontroleerde, waarmee nog nauwelijks rekening wordt gehouden. Bij een traditionele identiteitscontrole is de controleur de baas, hij heeft de regie en kan initiatieven nemen waarop de gecontroleerde moet *re*ageren. In digitale procedures of bij gebruik van digitale hulpmiddelen is de gecontroleerde echter de baas.
De precieze werking van de apparatuur zit voor de gemiddelde controleur 'onder de motorkap' en wordt doorgaans niet goed begrepen. Hij gaat dus af op het resultaat van de elektronische verificatie. Manipulatie daarvan merkt de controleur meestal niet op. Daarbij is ook nog eens het initiatief verschoven naar de identiteitsfraudeur, die actief een noodprocedure kan uitlokken, bijvoorbeeld door een pasje onbruikbaar te maken voor elektronische controle. De gecontroleerde heeft het verrassingseffect aan zijn kant en het is de controleur die moet *re*ageren. Een met opzet kapot gemaakte chip, bijvoorbeeld, geeft de fraudeur de zekerheid dat hij in de noodprocedure terechtkomt, zonder dat de controleur kan zien dat er opzet in het spel is. Bij de tenaamstelling van een (tijdelijk) document of bevoegdheid gaat de controleur vervolgens, bij gebrek aan beter, af op ongecontroleerde of oncontroleerbare gegevens en beweringen die de gecontroleerde hem aanreikt.

Dat brengt ons terug bij de eerste nieuwheidsfactor: een geslaagde identiteitsfraude wordt op het moment van de controle niet opgemerkt. Wie er het slachtoffer van wordt, krijgt het soms wel achteraf in de gaten. Maar dan is het te laat, omdat de dader niet meer te vinden is. Want eventuele sporen wijzen naar het slachtoffer.

Hoe erg is het? De casus 'strafrechtketen'

Hoe groot is het probleem van identiteitsfraude? Als geslaagde identiteitsfraudes niet gemakkelijk opgemerkt (kunnen) worden, is het ook niet eenvoudig om een beeld van de omvang van het probleem te krijgen. Er zijn maar weinig situaties waar de identiteitsfraudeur na een geslaagde identiteitsfraude niet kan ontsnappen. Een van deze situaties is de gevangenis. Als iemand een ander bereid heeft gevonden om tegen betaling zijn straf uit te zitten, treffen we de plaatsvervanger aan in de cel. Komt de persoonsverwisseling voortijdig aan het licht, dan gaat hij vrijuit. Hij heeft immers geen strafvonnis. Als de echte dader ook een alias heeft gebruikt, is hij meestal niet meer te achterhalen. En van een op het strafblad van iemand anders bijgeschreven vonnis heeft de werkelijke dader dan natuurlijk later geen last. Een loterij zonder nieten.
Laten we eens zien of we de omvang van het probleem van identiteitsfraude in de strafrechtketen indirect kunnen benaderen, rekening houdend met het gegeven dat geslaagde persoonsverwisselingen meestal onopgemerkt blijven. Het zou daarom kunnen gaan om het topje van de ijsberg. We kijken eerst naar het begin van de strafrechtketen: identiteitscontrole door de politie. Daarna kijken we naar het uiteinde van de strafrechtketen: identiteitscontrole door de detentie-inrichting bij insluiting en ontslag. Als aan het begin én het einde van de strafrechtketen afdoende met forensische biometrie de identiteit van verdachte en veroordeelde worden gecontroleerd, heeft het voor hem/haar nauwelijks meer zin om in tussenliggende schakels met de identiteiten te sjoemelen.

Begin van de strafrechtketen: identiteitscontrole door de politie

Meer dan 101.000 aantoonbare identiteitsfraudeurs zijn te vinden in het geautomatiseerde vingerafdrukkensysteem Havank van de Nederlandse politie. Dat is de oogst van zo'n vijftien jaar geautoma-

tiseerde forensische dactyloscopie. De slimsten onder hen blijken er volgens Havank gedurende die vijftien jaar zelfs tot 54 keer in geslaagd te zijn om de politie te misleiden met betrekking tot hun identiteit.
Hoe is het mogelijk dat op zulke schaal identiteitsfraude plaatsvindt in de strafrechtketen? In de praktijk van alledag vergeten politie en justitie kennelijk gemakkelijk dat zij in de strafrechtketen niet mogen rekenen op de medewerking van verdachten en veroordeelden. Er zijn veel mogelijkheden om de politie op een dwaalspoor te brengen. Bij aanhouding vraagt een politieman bijvoorbeeld een misdrijfverdachte hoe hij heet en controleert vervolgens in de Gemeentelijke Bevolkings administratie (GBA) of die gegevens kloppen. Dat blijkt natuurlijk het geval, ook als de verdachte iemand anders is. Legitimatie blijft soms achterwege, eventueel heeft de verdachte een 'geschikt' rijbewijs, met een op hem lijkende pasfoto, bij zich waarop de door hem opgegeven gegevens zijn vermeld. Als onze verdachte tegelijk bekent, blijft vingerafdrukcontrole met het Havank-systeem vaak achterwege, het misdrijf is immers al opgelost. Zo wordt het proces-verbaal, en later de dagvaarding, op de verkeerde naam gesteld. De verdachte kan ter zitting zijn bekentenis weer intrekken, want het strafrechtelijk onderzoek wordt meestal niet overgedaan. En na zijn veroordeling wordt het vonnis opgenomen in het strafblad met naam en nummer van degene op wiens identiteit de verdachte handig heeft meegelift. Dat kan degene betreffen die zich later met de oproepbrief bij de gevangenis meldt om (tegen betaling) de straf uit te zitten, of een onschuldig slachtoffer.

Registratie in Havank

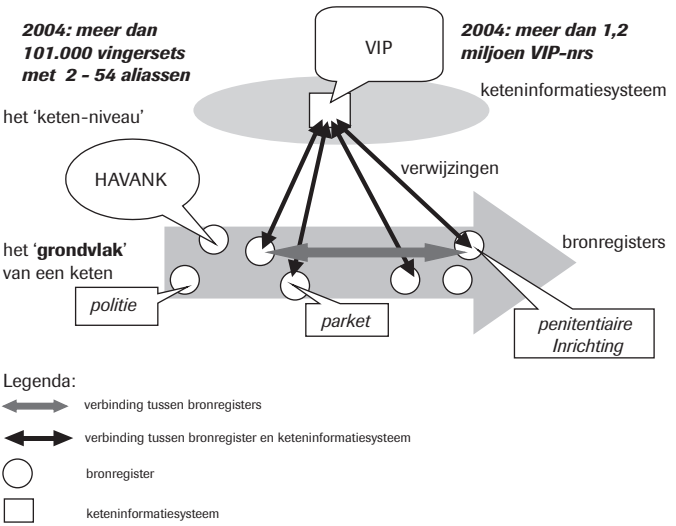
Bij de interpretatie van het kwantitatieve gegeven van de genoemde 101.000 vingerafdruksets met twee of meer administratieve identiteiten, moet men er rekening mee houden dat de politie de laatste jaren steeds minder vaak vraagt om vingerafdrukcontrole door de dactyloscopen van de dienst Nationale Recherche Informatie. Er past nog een tweede waarschuwing: alle andere sets vingerafdrukken in Havank met slechts één set identificerende persoonsgegevens kunnen eveneens op een alias zijn geregistreerd! Havank kijkt alleen naar de tien vingerafdrukken van een persoon en kan geen onderscheid maken tussen een ware identiteit en een

alias. De vingers kunnen wel van de echte dader zijn, maar het vonnis is door dat alias te gebruiken op het strafblad van iemand anders terechtgekomen. Als hij niet met dezelfde vingerset ook nog onder een andere naam in Havank zit, gaat men er bij Havank van uit dat naam en vingers bij elkaar horen, maar dat is natuurlijk niet vanzelfsprekend. Niet bij elk delict worden opnieuw vingerafdrukken afgenomen van een persoon die al bekend is bij de politie. Zou dit wel gebeuren, dan zou onmiddellijk blijken dat iemand zich voor een ander uitgeeft.

Het VIP-nummer

Behalve over Havank beschikt de strafrechtketen ook over een ketenbrede VerwijsIndex Personen strafrechthandhaving (VIP) die een uniek strafnummer, het VIP-nummer, toekent aan ieder die voor het eerst van een misdrijf wordt verdacht en die de opgegeven identificerende persoonsgegevens registreert. Als bovenstaande analyse juist is, zou men in VIP een vergelijkbaar beeld van identiteitsfraude moeten aantreffen. Als puur administratief systeem is VIP echter nauwelijks in staat aliasgebruik te constateren, maar met de Havank-gegevens die bij een VIP-nummer horen, kan dat wel. Zoals afbeelding 1 laat zien had de verwijsindex VIP van de strafrechtketen in 2004 al meer dan 1,2 miljoen VIP-nummers toegekend aan personen die in Compas voor het eerst van een misdrijf werden verdacht sinds de invoering van het aan de index gerelateerde ketennummerstelsel in 1993. Dat hoge aantal was aanleiding tot een steekproef waarbij VIP- en Havank-gegevens werden vergeleken. Bij dit onderzoek bleek bijvoorbeeld een van de VIP-nummers te relateren aan een Havank-nummer met 27 aliassen. Aan deze persoon bleken sinds 1993 in totaal 13 verschillende VIP-nummers te zijn toegekend, waarvan er 5 door de GBA correct waren bevonden. Door al deze VIP-nummers bij elkaar te brengen werd ook zichtbaar dat hij volgens de verwijsindex op dat moment op twee plaatsen in de gevangenis zat (bij latere controle bleek een van de twee intussen op vrije voeten te zijn gesteld).
Als identiteitsfraude in de strafrechtketen op zo'n grote schaal blijkt te kunnen plaatsvinden, waarom is dat dan zo erg? Aliassen in Havank zijn immers geen probleem voor het bewijzen van daderschap aan de hand van vingerafdrukken.

Afbeelding 1: HAVANK en VIP in de strafrechtketen



Als een op de plaats delict aangetroffen vingerafdruk van de vermoedelijke dader identiek blijkt te zijn aan de vingerafdruk van de verdachte, wijst dat biometrische gegeven door zijn aard naar de juiste persoon, ongeacht de naam die de verdachte heeft opgegeven. Het probleem zit dus niet in de strafrechtelijke bewijsvoering maar in de ketensamenwerking binnen de strafrechtketen. Het is gemakkelijk in te zien dat een verkeerde naam alle instanties in de rest van de strafrechtketen op het verkeerde been zet. Uiteindelijk wordt het strafvonnis zelfs in de verkeerde lade opgeborgen, zodat bijvoorbeeld verklaringen omtrent het gedrag eigenlijk een betrouwbare basis ontberen. Dat tast de bruikbaarheid van de rechtsorde aan. Overigens zet de politie zo ook zichzelf op het verkeerde been. Als bij een nieuw delict een vingerafdruk- of een DNA-spoor wordt gevonden dat kan worden gekoppeld aan een op een alias geregistreerde vingerafdruk of DNA-profiel, leidt dat tot onderzoek naar, of arrestatie van, de verkeerde persoon. Dat blijkt natuurlijk wel bij herhaalde DNA- of vingerafdrukcontrole, maar daar schiet de politie niet veel mee op.

Identiteitscontrole door de detentie-inrichting bij insluiting en ontslag

Terwijl er nu gewerkt wordt aan een betere wijze van identiteitscontrole van misdrijfverdachten door de politie aan het begin van de strafrechtketen, leek het ook nuttig om achter in de keten ook een steekproefonderzoek met vingerafdrukgegevens uit Havank te doen naar de identiteit van de actuele celbevolking in een gevangenis. Die steekproef was nodig, omdat in de gevangenissen geen routinecontrole met forensische vingerafdrukken (meer) plaatsvindt. Bij zelfmelders gaat men uit van de gegevens in de oproepbrief en bij aflevering van verdachten of veroordeelden door de politie op de door de politie aangeleverde gegevens.
In enkele detentie-inrichtingen werden 700 kort- en langgestrafte gedetineerden gecontroleerd. Een dergelijke ad hoc controle is echter een enorme logistieke operatie, die vier maanden voorbereidingstijd heeft gevergd en onmogelijk stil kon worden gehouden. Ondanks de lange voorbereidingstijd die in principe de gelegenheid bood om de controle te ontgaan, bleken van 46 gedetineerden de administratieve gegevens onjuist of bleek de persoon niet de juiste persoon te zijn, terwijl tevens bleek dat in een aantal gevallen de DNA-gegevens niet op de juiste persoon waren geregistreerd. Men zij echter voorzichtig met de interpretatie van de cijfers. Door de omstandigheden en lange voorbereidingstijd kan de pilot meting in drie gevangenissen nauwelijks een indicatie geven van de werkelijke omvang van identiteitsfraude achter in de strafrechtketen, hooguit een voorzichtige indicatie van de minimale omvang.
Als het zelfs onder de ogen van de strafwethandhavers gemakkelijk blijkt om zich van andere identiteiten te bedienen, mogen we ons geen illusies maken over de huidige omvang van identiteitsfraude in minder goed bewaakte maatschappelijke ketens, zoals de gezondheidszorg, de arbeidsmarkt, het onderwijs of het reisverkeer. Daarom is het de moeite waard om te verkennen aan welke eisen betere identiteitscontroles moeten voldoen en welke wapens de overheid tegen identiteitsfraude in stelling brengt.

Nieuwe oplossingsrichtingen voor effectieve identiteitscontroles

De huidige aandacht voor identiteitsbewijzen en voor de gegevens die daarop vermeld staan, speelt de identiteitsfraudeur in de kaart.

Hij wordt ook geholpen door onze rechtscultuur waarin identiteitscontroles in hoge mate voorspelbaar, uniform en observeerbaar zijn geworden. Voorspelbaarheid, uniformiteit en openbaarheid zijn geen bezwaar voor de bestrijding van valse identiteitsdocumenten, maar vormen minder geschikte uitgangspunten voor de bestrijding van identiteitsfraude.

Effectieve bestrijding van identiteitsfraude vereist dat de voorspelbaarheid van identiteitscontroles drastisch wordt verminderd, bijvoorbeeld door verschillende controleprocedures met wisselende persoonsgegevens afkomstig uit een onafhankelijke bron. Dit vereist naast aandacht voor identiteitsbewijzen en persoonsnummers, méér aandacht voor:

– *de persoon die er zich van bedient*

De identiteit van een persoon kan beter worden gecontroleerd met gegevens die alleen de betrokkene kan kennen of met vragen waarop alleen de juiste persoon spontaan kan antwoorden zonder uit zijn rol te vallen. De gebruikelijke pasfoto lijkt wel persoonsgericht, maar is te klein en te vaag om personen effectief te kunnen controleren. Hoge resolutie pasfoto's die op een beeldscherm sterk kunnen worden vergroot zonder verlies van scherpte, blijken voor visuele controle beter te voldoen.

– *geschikte controlegegevens*

Geschikte controlegegevens kunnen overal vandaan komen, mits ze voor derden met kwade bedoelingen niet van tevoren voorspelbaar of bekend zijn. Dat is situatieafhankelijk. In een ziekenhuis kan een eerder consult als controlegegeven worden gebruikt, mits dit in de ziekenhuisadministratie gemakkelijk is terug te vinden. Bij grenspassage kan men denken aan de laatste pinbetaling voordat men incheckte. Deze controlegegevens kunnen ook door of bij een andere instantie worden geverifieerd, in dit voorbeeld door Interpay. Het gaat hier niet om een vrije online toegankelijkheid van het controlegegeven, maar om een beveiligde geautomatiseerde toegang op basis van een strakke en hoogdrempelige autorisatie, waarbij de uitslag van de controle wordt teruggegeven zonder het controlegegeven zelf vooraf prijs te geven. De harde noodzaak om een identiteit te beschermen tegen meeliften en diefstal eist onafhankelijke controlegegevens. Aan de Universiteit Utrecht loopt momenteel een onderzoek naar de vraag welke sporen mensen in het maatschappelijk verkeer achterlaten en hoe die als onafhankelijk controlegegeven zouden kunnen dienen binnen de grenzen

van de wet. De op een identiteitsbewijs vermelde identificerende persoonsgegevens en persoonsnummers zijn in ieder geval niet geschikt voor *identiteits*controle, omdat deze bij de identiteitsfraudeur bekend zijn en door de gecontroleerde worden meegebracht. De hier bedoelde maatwerkaanpak op het moment van controle van een persoon verdient in ieder geval de voorkeur boven het creëren van één grote databank met allerlei controlegegevens met betrekking tot alle te controleren personen die ook voor allerlei andere doeleinden zouden kunnen worden gebruikt. Gezien onze gebrekkige kennis van grootschalig gegevensgebruik en onze onbekendheid met de verdere ontwikkeling van de wereldomspannende informatiesamenleving is die oplossingsrichting op dit moment niet verantwoord.

– *het proces van identiteitscontrole*

Elke situatie van identiteitscontrole is anders, afhankelijk van de context waarin deze plaatsvindt. Per situatie vertegenwoordigt een geslaagde identiteitsfraude een andere sociale en economische waarde, zijn andere aanvullende controlegegevens het meest geëigend en zijn de kansen op preventie van identiteitsfraude verschillend. Elke situatie heeft bovendien eigen fall-back procedures voor gevallen waarin de standaardcontrole niet werkt. Omdat deze doorgaans lichter uitvallen, hebben ze voor kwaadwillenden een aanzuigende werking. Een identiteitscontrole is dus maatwerk. Voorspelbare uniforme procedures tasten de doeltreffendheid van elke identiteitscontrole aan.

– *de waarde van identiteitsinstrumenten*

Door gestandaardiseerde uniforme, openbare en algemeen bruikbare identiteitsbewijzen en vermelding daarop van een verplicht te gebruiken algemeen persoonsnummer zijn onze identiteitsinstrumenten voor de identiteitsfraudeur zeer waardevol geworden. We dienen in de toekomst manieren te vinden om die waarde te verkleinen. Dat kan bijvoorbeeld door de bruikbaarheid van een identiteitsinstrument voor niet-rechthebbenden te beperken door toevoeging van een pincode, of door combinatie met ketennummers of proceduregebonden transactiecodes.

In de toekomst mogen identiteitsfraudeurs dus niet meer van tevoren kunnen weten waar, wanneer en hoe ze tegen de lamp zullen lopen. De grootste hefboomwerking mag verwacht worden van verrassingseffecten en gevarieerde procedures. Met geheime

controle-instructies kunnen identiteitscontroles gevarieerder en voor de identiteitsfraudeur minder voorspelbaar worden gemaakt. Voor het doel van identiteitscontrole hoeft dit niet tegen de wet te zijn, omdat externe instructies volgens art. 10 lid 2 van de Wet Openbaarheid Bestuur (WOB) niet openbaar hoeven te worden gemaakt als een van de uitzonderingscriteria van toepassing is. Te denken valt aan de uitzonderingscriteria 'de opsporing en vervolging van strafbare feiten' en 'inspectie, controle en toezicht door bestuursorganen'. Volgens jurisprudentie door de Hoge Raad is voor het eerstgenoemde criterium niet noodzakelijk dat er van een concrete verdenking sprake is. Onder dit criterium kunnen dus ook algemene instructies vallen voor identiteitscontroles die voor de gecontroleerde minder voorspelbaar verlopen.

Welke wapens brengt de Nederlandse overheid in stelling?

Identiteitsfraude dwingt ons dus tot een nieuwe kijk op kaders, functie en gebruik van identiteitsinstrumenten in onze rechtscultuur. Instrumenten die voor bestrijding van gebruik van valse of vervalste identiteitsbewijzen nuttig zijn, blijken dat niet te zijn voor bestrijding van identiteitsfraude. Vaak werken ze zelfs averechts, door de wijze waarop ze worden ingezet. Ook informatietechnologie voor identiteitscontroles komt in een ander licht te staan. Desondanks blijven we een naïef vertrouwen koesteren in technologie en administratie.
Identiteitsfraude kan men zien als een verschijnsel dat identiteitsbeheer en identiteitscontroles complexer maakt en dat als reactie daarop bestuurlijke maatregelen uitlokt om greep te houden op de toegenomen complexiteit. Te denken valt in dit kader aan een chip op het paspoort, een algemeen verplicht persoonsnummer en biometrie op het identiteitsbewijs, inclusief de ermee verbonden werkwijzen. Doel van deze maatregelen is in de eerste plaats het *reduceren* van de toegenomen complexiteit. Deze juridisch-bestuurlijke aanpak wordt gekenmerkt door een uitgesproken voorkeur voor eenvoud, uniformiteit, openbaarheid en transparantie. Gezien vanuit de eisen van openbaar bestuur is daar niets mis mee. Integendeel, ordening is gebaat bij kenbaarheid en overzichtelijkheid van de informatie, eenvoudige uniforme instrumenten en voorspelbare gestandaardiseerde werkwijzen. Daar staat wel tegenover dat deze aanpak onze identiteits-

controles stap voor stap meer overzichtelijk, uniform en voorspelbaar heeft gemaakt ten faveure van de identiteitsfraudeur. Deze juridisch-bestuurlijke aanpak staat in schril contrast tot wat levende organismen in de natuur doen wanneer hun omgeving complexer wordt. Die kiezen niet voor reductie van complexiteit, maar juist voor het tegendeel. Ze passen zich aan door zichzelf ook complexer te maken, onder andere met behulp van toenemende interne differentiatie, meer variatie in gedrag en vooral met extra feedbackmechanismen. Kennelijk is bij toegenomen omgevingscomplexiteit in de natuur beter waarnemen het begin van beter beheersen. Vereenvoudiging of standaardisatie van instrumenten en vergroting van voorspelbaarheid of transparantie van werkwijzen leveren het tegendeel op, vooral minder waarnemingsmogelijkheden en minder feedbackmechanismen. Ook voor identiteitscontroles.

Drie voorbeelden van nieuwe beleidsmaatregelen ter verbetering van identiteitscontroles

Het biometrische paspoort

Ter bestrijding van een bepaalde vorm van identiteitsfraude, namelijk gebruik van een paspoort door iemand die op de houder lijkt (lookalike fraude), is een wetsontwerp bij de Tweede Kamer ingediend tot wijziging van de Paspoortwet om een biometrisch kenmerk (bijvoorbeeld een vingerafdruk) op het nieuwe Nederlandse paspoort te kunnen zetten. Op dezelfde manier als sinds 1996 het sofi-nummer op identiteitsbewijzen wordt vermeld. Voordeel hiervan is dat daarmee in situaties waarin een identificatieplicht geldt biometrische identiteitscontrole mogelijk wordt met het paspoort, dat bij ons het belangrijkste wettelijke identiteitsbewijs is. Daarmee wordt de paspoortbiometrie de facto de algemene standaard voor biometrische identiteitscontrole in Nederland, net zoals het sofi-nummer sinds 1996 geleidelijk de rol van algemeen persoonsnummer is gaan vervullen. Nadeel van de vermelding van een persoonsnummer of een biometrisch kenmerk *op* een document met persoonsidentificerende gegevens is, dat het de fraudeur onbedoeld gemakkelijk wordt gemaakt. Hij weet immers van tevoren dat elke nummer-naamcontrole slaagt, ook als hij het identiteitsbewijs van iemand anders gebruikt. Zo weet hij in de toekomst ook aan

welke meetwaarde zijn biometrische meting moet beantwoorden. Die blijkt op verschillende manieren na te bootsen of na te maken. Ook kan men op verschillende manieren de meting frustreren waardoor men in een noodprocedure komt waarin men zich met enige voorbereiding voor iemand anders kan uitgeven. Proefnemingen wijzen uit dat de huidige biometrische apparatuur gemakkelijk is te misleiden. Dat staat los van het groeiende besef dat we nog niet in staat zijn een grootschalige toepassing van biometrie voldoende fraudebestendig te organiseren. Techniek en organisatie samen moeten de veiligheid en betrouwbaarheid kunnen garanderen. Dat is momenteel beslist niet het geval. De identiteitsfraudeur kan dus met geduldige observatie de zwakke plekken in identiteitscontroles ontdekken en een werkwijze uitdenken die hem de grootste kans op succes garandeert. Als hij wordt betrapt, blijft dat vrijwel altijd zonder gevolgen. Zo levert nieuwe technologie onbedoeld vaak het omgekeerde op van wat ervan wordt verwacht: in plaats van een betere identiteitscontrole, méér identiteitsfraude!

De harde noodzaak om in de toekomst een identiteit afdoende te beschermen tegen meeliften en diefstal stelt ook speciale eisen aan de inzet van biometrie, vooral bij gebruik van een onveranderlijk biometrisch kenmerk zoals een vingerafdruk. Door de vingerafdruk, beveiligd of niet, op het identiteitsbewijs te zetten is het geen onafhankelijk controlegegeven meer en is off line gebruik fraudegevoelig. Bij gebruik van biometrische kenmerken op grote schaal is de beveiliging ervan bij de huidige stand van de technologie ondoenlijk. Dit kan in de toekomst veranderen. Aan de Universiteit Utrecht wordt bijvoorbeeld momenteel onderzocht of er een vingerafdruk kan worden geconstrueerd die samengesteld is uit gedeelten van de afdrukken van meerdere vingers van dezelfde persoon. Die zou eventueel wel op een document kunnen worden gezet, omdat namaken van die niet bestaande vingerafdruk weinig zinvol is, terwijl alleen de juiste persoon alle vingers bij zich heeft.

Vanuit het perspectief van identiteitsfraude is het nu nog beter om de biometrische verificatie op afstand te laten doen op het moment van identiteitscontrole door uitgever van het identiteitsbewijs, mits goed beveiligd en strak bewaakt. Deze oplossing kan zowel misbruik door gecontroleerde als door de controleur tegengaan. Een pincode en het documentnummer samen kunnen daarbij dienen als koppelmechanisme naar het relevante biometrische gegeven dat elders veilig is opgeslagen. Daarbij gelden dezelfde normen als bij

andere controlegegevens. Geen grote on line vrij bevraagbare databank met alle biometrische gegevens van de hele bevolking, waarbij het opgeslagen biometrische gegeven zelf wordt prijsgegeven.
Een databank is wel beter te beveiligen dan een document, maar ook hier liggen risico's op de loer die pleiten voor onafhankelijke gemeentelijke databanken met een kleine centrale component voor beveiliging en fraudebestrijding. De geautomatiseerde biometrische controle wordt dan vanuit de gemeente verricht, zonder het opgeslagen kenmerk prijs te geven en zonder op enigerlei andere wijze aan buitenstaanders toegang te verlenen tot die databank. Hiervoor zijn natuurlijk andere vingerafdrukken nodig dan die welke op het identiteitsbewijs staan, want die kan men niet meer gebruiken. Indien men een paspoortvinger kan nabootsen of namaken, wordt ook de controle op afstand misleid.
Vandaar dat de ministers van Justitie, Vreemdelingenzaken en Integratie en Bestuurlijke Vernieuwing in 2004 hebben afgesproken dat ten minste een derde vingerafdruk zal worden opgeslagen in de gemeentelijke reisdocumentenadministratie, naast de twee vingerafdrukken die volgens de EU-afspraken op het document moeten worden vermeld. Afgesproken is ook dat op elke lokatie waar identiteitscontrole verplicht is, biometrische controle op afstand mogelijk moet zijn.
Deze afspraken maken het mogelijk de feitelijke werkwijze voldoende onvoorspelbaar te maken, zodat veel identiteitsfraudeurs zullen worden afgeschrikt. Op deze wijze kan de overheid de identiteit van de eigen burgers redelijk beschermen tegen meeliften en identiteitsdiefstal. Niet voldoende, want bescherming tegen misbruik buiten Nederland van de biometrische kenmerken die op het identiteitsbewijs staan is ondoenlijk. Vingerafdrukken, beveiligd of niet, horen daarom eigenlijk niet thuis op een reisdocument dat bedoeld is om overal ter wereld, ook in minder betrouwbare omgevingen, voor allerlei doeleinden te overhandigen.
Als in het buitenland biometrische identiteitsfraude met Nederlandse identiteiten de kop gaat opsteken, zullen we ongetwijfeld op deze schreden terugkeren. Hopelijk hebben we op dat moment de infrastructuur die nodig is om op afstand een biometrische identiteitscontrole te (laten) doen, al enigszins op orde. Vandaar de hierboven geschetste tweeledige Nederlandse koers, die echter op EU-niveau nog niet is geaccepteerd. Daar overheerst het privacydebat.

Privacypleitbezorgers willen biometrische kenmerken alléén op het document zetten dat met de houder wordt weergegeven, omdat dat een betere bescherming van de privacy van de houder zou opleveren. Centrale opslag waarbij alle biometrische gegevens on line voor elke controleur toegankelijk zijn, wordt als te bedreigend beschouwd. Het laatste punt lijkt mij juist, maar hierboven heb ik een verantwoord alternatief geschetst. Het eerste punt is niet juist. Men realiseert zich onvoldoende dat een biometrische identiteitsdiefstal een enorme en permanente privacybedreiging oplevert, terwijl men die op deze wijze gemakkelijker maakt. Men houdt onvoldoende rekening met de veiligheidsrisico's die kleven aan wereldwijd gebruik van een biometrisch kenmerk, gegeven de enorme voordelen van identiteitsfraude en het gigantische handhavingstekort bij grensoverschrijdende identiteitsfraude.

Het burgerservicenummer (BSN)

Het tweede voorbeeld van een nieuwe beleidsmaatregel om identiteitscontroles te verbeteren vormt het voornemen van de Nederlandse regering om een verplicht openbaar algemeen persoonsnummer in te voeren, het zogenaamde burgerservicenummer (BSN). Persoonsnummers zijn geleidelijk een belangrijke rol gaan vervullen, zowel bij het administratief koppelen en afschermen van persoonsgegevens, als bij het herkennen van personen. Dat heeft ertoe geleid dat misbruik van persoonsnummers een steeds belangrijker vorm van identiteitsfraude wordt. Vanuit de traditionele juridisch-bestuurlijke benadering ligt het voor de hand om als tegenmaatregel een algemeen openbaar persoonsnummer in te voeren dat:

– *verplicht in allerlei situaties moet worden gebruikt*, ongeacht de te ondersteunen processen en ongeacht de specifieke problemen die men in een bepaalde situatie met het persoonsnummer wil oplossen (dit weerspiegelt het juridisch-bestuurlijk streven naar eenvoud, uniformiteit en voorspelbaarheid);
– *op alle wettelijke identiteitsbewijzen moet worden vermeld* (dit weerspiegelt het juridisch-bestuurlijk streven naar uniformiteit, openbaarheid, en kenbaarheid).

Bestrijding van identiteitsfraude, daarentegen, eist in de toekomst eigenlijk een meer gedifferentieerd persoonsnummerbeleid, waarbij een aantal verschillende en onafhankelijk van elkaar beheerde

sectornummers worden gebruikt die, indien nodig en met inachtneming van passende procedures, met elkaar kunnen worden vergeleken. Een algemeen persoonsnummer is daarbij nuttig om sectorale persoonsnummers te koppelen om zo identiteitsfraude gemakkelijker aan het licht te brengen. Daarom mag een algemeen persoonsnummer de sectorale persoonsnummers niet aantasten of verdringen. Dat betekent dat een algemeen persoonsnummer niet verplicht en niet openbaar mag zijn, en niet mag worden verspreid of gebruikt voor externe communicatie. Enkele verschillende sectorale persoonsnummers bieden controlemogelijkheden en maken feedbackmechanismen mogelijk. De sectorale persoonsnummers zijn minder kwetsbaar voor vervuiling, disfunctioneren, fouten en fraude, omdat ze elk voor zich minder belangrijk en waardevol zijn, en daarmee minder aantrekkelijk voor de identiteitsfraudeur. Het wordt voor de fraudeur bovendien – in vergelijking met een situatie met slechts één algemeen persoonsnummer – moeilijker te voorspellen wanneer, waar en hoe hij tegen de lamp zal lopen, omdat hij niet kan overzien welke andere persoonsnummers hij allemaal consistent met elkaar moet houden om niet op te vallen.
Verplicht algemeen gebruik van één algemeen openbaar persoonsnummer zoals het toekomstige BSN, daarentegen, maakt dit persoonsnummer onvermijdelijk erg waardevol, zodat dit extra kwetsbaar wordt voor oneigenlijk gebruik, fouten en fraude. Omdat er door het verplichte algemene gebruik minder sectornummers in stand zullen blijven die op zich als controlegegeven kunnen dienen, of als toegang tot aanhangende persoonsgegevens, nemen tegelijkertijd de controlemogelijkheden af. Dat is een groot nadeel omdat juist een algemeen persoonsnummer meestal moeilijk te beheren is. Dat komt omdat nummerbeheer zich eigenlijk moet richten op de risico's in de meest kritische sector. Maar draagvlak voor de extra kosten hiervan ontbreekt vaak in andere meegebruikende sectoren, zodat per saldo met een minimale beheersinspanning moet worden volstaan.
De keuze voor een verplicht algemeen openbaar persoonsnummer lijkt dus op het oog aantrekkelijk, maar daar staat tegenover dat de bestrijding van identiteitsfraude en van inbreuken op de persoonlijke levenssfeer moeilijker wordt door gebrek aan onafhankelijke controlegegevens.

Identificatieplicht in ziekenhuizen

Het laatste voorbeeld betreft de invoering van de identificatieplicht in de gezondheidszorg per 1 januari 2006. Aanleiding vormden sterke aanwijzingen dat identificatie met de pasjes van de zorgverzekeraar ruimte liet voor gesjoemel op grote schaal (Grijpink, 2002). Ziekenhuizen en poliklinieken die nu nalaten de identiteit van hun patiënten te controleren, zullen hun kosten niet langer bij het ziekenfonds kunnen declareren.
Ook in dit derde voorbeeld is sprake van een onderschatting van de fraudeproblematiek. Het gaat meestal niet om vervalste zorgpasjes, maar om identiteitsfraude, namelijk lookalike fraude. Je kunt je afvragen of het zal helpen als de pasjes beter worden gecontroleerd met gebruik van wettelijke identiteitsbewijzen. Medewerkers in de gezondheidszorg zijn op dat gebied niet deskundig. Het middel is misschien wel erger dan de kwaal, als via deze identificatieplicht het op grote schaal misbruikte sofi-nummer (identiek aan het toekomstige BSN) zou inburgeren als toegang tot het (elektronisch) medisch dossier. De minister van VWS heeft besloten dat het BSN zal dienen als Zorg Identificatie Nummer (Zin) zodra dit officieel bij wet als verplicht nationaal persoonsnummer is ingevoerd. Meeliften op een BSN van iemand anders zal dan in de toekomst automatisch leiden tot gebruik van de medische gegevens van die persoon, terwijl nieuwe gegevens weer in dat dossier worden gearchiveerd. Het BSN als Zin zal op termijn een vrijwel niet meer herstelbare chaos in de medische dossiers teweegbrengen, met veel medische fouten en onderbehandeling als gevolg.

Conclusies en aanbevelingen

Het ziet er op dit moment dus naar uit dat de Nederlandse overheid, in het kielzog van de Europese Unie, enkele maatregelen in petto heeft die identiteitsfraude eerder gemakkelijker dan moeilijker zullen maken en die de nadelige gevolgen van geslaagde identiteitsfraude drastisch zullen vergroten.

Identiteitsfraude

Het verdient aanbeveling om bij voorrang de identiteitsfraude in de strafrechtketen bij de kop te pakken, ook om ervaring op te doen met grootschalige schoonmaak van kernregisters in een keten. Als daarna(ast) de identiteitsketen aan de orde komt, is het van belang burgers die menen dat ze het slachtoffer van identiteitsfraude zijn, een laagdrempelig meld- en onderzoekcentrum te bieden, zodat we ervaring kunnen opdoen met werkwijzen waarmee je beter kunt vaststellen of iemand een slachtoffer of een dader is. Identiteitscontroles dienen anders te worden ingericht, waarbij het vooral van belang is dat minder voorspelbaar wordt hoe de identiteitscontrole plaats zal vinden.

Biometrie

Als de overheid biometrie in wil zetten, verdient het aanbeveling deze biometrie gescheiden van de forensische biometrie te ontwikkelen en te beheren. Identiteitscontroles dienen zo te worden ingericht, dat gelijktijdig van meerdere biometrische gegevens of technieken gebruik wordt gemaakt, omdat die moeilijk gelijktijdig consistent te manipuleren zijn. Voor de paspoortbiometrie dienen een of twee andere vingerafdrukken dan die op het paspoort staan beschikbaar te zijn in achterliggende gemeentelijke reisdocumentenadministraties, om op afstand een eigen inwoner biometrisch te kunnen controleren. Dat maakt het tevens voor de fraudeur onzeker of hij kan volstaan met het manipuleren van de vingerafdrukcontrole met de vingerafdrukken die op het identiteitsbewijs staan. Zolang we weinig ervaring hebben met grootschalige toepassing van biometrie, verdient kleinschalige toepassing meer aandacht. Binnengemeentelijk gebruik van vingerafdrukken in het kader van de aanvraag- en verstrekkingsprocedure van paspoorten en identiteitsbewijzen en als biometrisch anker van digitale foto en handtekening van de houder, zou identiteitsfraude al fors bemoeilijken. Daarvoor hoeven geen vingerafdrukken op het document te worden meegegeven. Hiermee is al een grote mate van bescherming van Nederlandse identiteiten tegen identiteitsfraude door binnen- en buitenlandse meelifters mogelijk.

Persoonsnummers

Met betrekking tot een algemeen nationaal persoonsnummer (BSN) is het advies te voorkomen dat overheidsinstanties zich belemmerd zouden voelen om voor algemene preventie van identiteitsfraude ook andere persoonsnummers en persoonsgegevens te gebruiken. Verplicht uitsluitend gebruik van een BSN voor koppeling van gegevens binnen de overheid. Onderlinge communicatie tussen overheidsinstanties enkel op basis van een BSN is dus uit den boze. Voorzieningen waarbij de identiteit van burgers elektronisch eenmalig wordt geverifieerd zonder dat de uitvoerende instanties de identiteit van de burger zelf mogen onderzoeken door opnieuw naar essentiële controlegegevens te vragen, dienen niet te worden ingevoerd. Ìndien men per se persoonsnummers op documenten wil vermelden, is het vanuit perspectief van identiteitsfraudepreventie beter om slechts een gedeelte van het nummer te vermelden. Dat is voldoende als koppelgegeven en dwingt tot het gebruik van een andere, bij voorkeur onafhankelijke bron. Dat belemmert in ieder geval het meeliften op iemands persoonsnummer, door overlegging van een fotokopie van diens (gestolen of geleende) identiteitsbewijs.

Literatuur

Ashbourn, J.
Practical biometrics; from aspiration to implementation
London, Springer-Verlag, 2004

Baum, K.
Identity theft, 2004
US Department of Justice, Office of Justice Programs, April 2006, NCJ 212213

Grijpink, J.H.A.M.
Identiteit als kernvraagstuk in een informatiesamenleving
In: *Handboek Fraudepreventie*, hoofdstuk Fraude en integriteit, nr. E 4010, Samson, Alphen aan den Rijn, 1999

Grijpink, J.H.A.M.
Biometrie en privacy
Privacy & Informatie, nr. 6, , Koninklijke Vermande, 2000

Grijpink, J.H.A.M.
Checklist Preventie van risico's van chipkaarttoepassingen
Checklisten Informatiemanagement, Ten Hagen Stam, Den Haag, november 2000, rubriek 1.F.14

Grijpink, J.H.A.M.
Persoonsnummers en privacy
Privacy & Informatie, 5e jrg., nr. 2, 2002, p. 52-56, 2002 en 3, 2002, p. 100-105

Grijpink, J.H.A.M.
Informatiestrategie voor ketensamenwerking
Den Haag, Sdu Uitgevers, 2002

Grijpink, J.H.A.M.
Identiteitsfraude als uitdaging voor de rechtstaat
Privacy & Informatie, 6e jrg., nr. 4, 2003, p. 148-153

Grijpink, J.H.A.M.
Two barriers to realizing the benefits of biometrics; a chain perspective on biometrics, and identity fraud as biometrics' real challenge
Computer law and security report, 21e jrg., nr. 2 en 3, 2005, p. 138-145; 249-256

Grijpink, J.H.A.M.
Een beoordelingsmodel voor de inzet van biometrie
Privacy en Informatie, 9e jrg., nr. 1, 2006, p. 14-17

Grijpink, J.H.A.M.
Criminal records in the European Union; the challenge of large-scale information exchange
European journal of crime, criminal law and criminal justice, 14e jrg., 2006, p. 1-19

McDonald, Ph. e.a.
A national strategy to combat identity theft
John Hopkins University in cooperative agreement with the US Department of Justice, Office of Community Oriented Policing Services, May 2006, ISBN 1-932582-64-9

Menn, J.
ID theft infects medical records
LA Times, 25 September 2006

Meulen, N. van der
The challenge of countering identity theft; recent developments in the United States, the United Kingdom, and the European Union
Report Commissioned by the National Infrastructure Cyber Crime program (NICC), International Victimology Institute Tilburg, 6 September 2006

SIOD (Sociale Inlichtingen en Opsporingsdienst)
Beleidsdocument 'Labyrint', onderzoek naar West-Afrikaanse criminele netwerken in de sociale zekerheid
Den Haag, Ministerie van Sociale Zaken, 2005