ICT ALS STRATEGISCHE UITDAGING

Een beoordelingsmodel voor de inzet van biometrie[1]

Prof. dr mr Jan Grijpink[2]

Samenvatting

Introductie van nieuwe technologie plaatst ons steeds vaker voor strategische vraagstukken omdat de onbedoelde averechtse neveneffecten vaak te laat zichtbaar worden. Een meer systematische en preventieve benadering is daarom wenselijk. Daarvoor wordt hieronder een speels beoordelingsmodel geschetst. Het gebruik van dit model wordt toegelicht aan de hand van de voorgenomen inzet van biometrie bij de bestrijding van identiteitsfraude in maatschappelijke processen (de zogenaamde paspoortbiometrie). Dat voorbeeld maakt duidelijk, dat het model een nuttig stuk gereedschap kan vormen. Het gekozen voorbeeld heeft bovendien betrekking op een van de belangrijkste scharnierpunten van maatschappelijke processen: over wie gaat het eigenlijk? Als we daar ICT voor inzetten, zitten we niet op averechtse effecten te wachten.

1. Beoordelingsmodel voor inzet van ICT

Nieuwe technologie passen we toe vanuit de gangbare kijk op de problematiek die we ermee willen oplossen. Omdat we ICT inzetten vanuit hetzelfde denkkader dat het probleem heeft doen ontstaan of de aanpak heeft geblokkeerd, maakt ICT-inzet het probleem daarom vaak eerst groter. Dat noem ik 'ICT als spelbederver'. Analyse van dat spelbederf brengt ons op het spoor van andere denkkaders die laten zien hoe ICT wel kan bijdragen aan een oplossing. Die rol van ICT noem ik die van 'dwarskijker'. In dit beoordelingsmodel is ICT dus zowel spelbederver als dwarskijker. Bekijk ICT als spelbederver en je kunt analyseren hoe het spelbederf ontstaat. Bekijk ICT als dwarskijker, dan zie je hoe je spelbederf kunt indammen.

Eerst een vingeroefening om het model te illustreren (het echte voorbeeld volgt hieronder). We zien ICT doorgaans vooral als een middel om gegevens geautomatiseerd te verzamelen, vast te leggen en te verwerken. Deze inzet van ICT in de publieke sector leidt zo spontaan tot aparte geautomatiseerde gegevensverzamelingen voor elk maatschappelijk vraagstuk (criminele vreemdelingen, verslaafde arrestanten, pedofiele buurtbewoners, veelplegende criminele jongeren, gevaarlijke reizigers, etc). Het gevolg hiervan is een steeds chaotischer lappendeken van moeilijk beheer(s)bare gegevensverzamelingen. Het spelbederf tekent zich af! Analyse van het spelbederf kan ons op het spoor brengen van andere denkkaders en benaderingen. Eigenlijk willen we een overheid die in actie komt als dat nodig is en dan de juiste beslissingen neemt. Dat eist bij de inzet van ICT meer aandacht voor geautomatiseerd communiceren tussen organisaties in maatschappelijke ketens. De dwarskijkrol van ICT suggereert dus méér ketencommunicatie[3], om de nadelige effecten van de voortschrijdende digitalisering in maatschappelijke processen op te vangen. Binnen en tussen maatschappelijke ketens blijkt op snelle en doeltreffende wijze informatie te kunnen worden uitgewisseld, zonder de privacy van burgers aan te tasten. Het belang daarvan zal in de toekomst verder toenemen naarmate in het kader van internationale samenwerking meer en vaker persoonsgegevens moeten worden uitgewisseld met instanties in rechtsculturen die minder garanties bieden voor wat in onze ogen rechtmatig gebruik van persoonsgegevens is. Daar is wel een andere benadering dan de gebruikelijke voor nodig, het alternatieve denkkader volgens het model. Het besef dat ICT eerst de rol van spelbederver speelt, kan er voor zorgen dat we het spelbederf zo kort mogelijk laten duren, en de negatieve gevolgen ervan zo klein mogelijk houden.

2. Toepassing van het model op paspoortbiometrie

Het voorbeeld om het beoordelingsmodel mee toe te lichten betreft de inzet van biometrie als wapen in de strijd tegen identiteitsfraude in maatschappelijke processen. *Identiteitsfraude* wil hier zeggen dat iemand met kwade bedoelingen bewust de schijn oproept van een identiteit die niet bij hem hoort[4]. Dit kan een bestaande identiteit van iemand anders zijn of een gefingeerde identiteit. Deze begripsomschrijving van identiteitsfraude is ruimer dan de gangbare die zich beperkt tot fraude met een officieel identiteitsbewijs (paspoort, identiteitskaart, rijbewijs). In de gangbare, beperkte benadering wordt er onvoldoende rekening mee gehouden, dat de voortschrijdende digitalisering het mogelijk maakt ook persoonsnummers, foto's, handelingen of gebeurtenissen te gebruiken, omdat mensen ook daaruit conclusies trekken over wie ze tegenover zich hebben. Identiteitsfraude in de bredere betekenis vindt daarom overal en op allerlei manieren plaats, en is niet beperkt tot specifieke situaties, procedures of documenten. Als een persoonsverwis-

seling eenmaal ergens is geslaagd, kan ze daarna langs reguliere wegen doorwerken op diverse andere situaties. Daar kan men de voorafgaande frauduleuze persoonsverwisseling vaak niet meer doorzien. De voortschrijdende digitalisering van de samenleving maakt identiteitsfraude steeds gemakkelijker. Het nieuwe van identiteitsfraude is dat geslaagde identiteitsfraude wél steeds meer sporen in de digitale omgeving achterlaat, maar dat die sporen naar het slachtoffer leiden in plaats van naar de dader! Daarom is het slachtoffer de eerste en vaak enige verdachte, die zich vervolgens niet of met moeite kan zuiveren van deze onterechte verdenking. Zijn bewijspositie is ook meestal onmogelijk, omdat hij moet bewijzen dat hij iets niet heeft gedaan.

Omdat identiteitsfraude aan de basis ligt van veel georganiseerde criminaliteit en terrorisme wordt momenteel in veel landen overwogen om identiteitsbewijzen en reisdocumenten te voorzien van een biometrisch kenmerk van de houder. Met *biometrie* wordt bedoeld dat men kenmerken van het lichaam (bijvoorbeeld de vingerafdruk of de stem) gebruikt als digitale sleutel om iemand elektronisch te herkennen, of om toegang te krijgen of te geven tot processen of gegevens. Ook private organisaties zullen biometrie gaan inzetten, omdat biometrische kenmerken de enige persoonsgebonden gegevens zijn met een fysieke relatie tot natuurlijke personen. Alleen een biometrische identiteitscontrole maakt gebruik van deze lichaamsgebonden kenmerken om vast te stellen op wie een document, een voorwerp of een gegeven betrekking heeft. Gebruik van andere gegevens levert alleen administratieve controles op[5]. Biometrie en biometrische identiteitscontrole zullen daarom geleidelijk een dominante plaats krijgen in allerlei kritische maatschappelijke processen, naarmate de digitalisering verder voortschrijdt. De paspoortbiometrie levert zo een mooi voorbeeld op van de inzet van nieuwe ICT om het hier geschetste beoordelingsmodel te illustreren.

3. Het spelbederf van de paspoortbiometrie

Het plan is nu om biometrie (vingerafdrukken) toe te voegen aan de persoonsgegevens *op* het paspoort en de identiteitskaart. Dit is logisch vanuit het gebruikelijke bestuurlijke denkkader, met transparantie en overzichtelijkheid in de hoofdrol. Men beseft daarbij niet, dat juist deze benadering in het verleden identiteitsfraude de kans heeft gegeven uit de hand te lopen. In 1996 is in Nederland immers op vergelijkbare wijze het sofi-nummer *op* paspoort en rijbewijs gezet. Dat heeft tot een sterke toename van identiteitsfraude geleid[6]. Deze bestuurlijke benadering voldoet alleen, als het identiteitsbewijs deugt en de houder de juiste persoon is. Niet, als het identiteitsbewijs wordt gebruikt door iemand die alleen maar op de rechtmatige houder lijkt. Dan kan iemand ongemerkt diens identiteit aannemen en bijvoorbeeld op diens sofinummer meeliften. De gangbare ‘naam-nummer’-controle op basis van een identiteitsbewijs is daar niet op berekend. In veel controlesituaties kan bovendien worden volstaan met het overleggen van een kopie van dat identiteitsbewijs waarmee ook nog gemakkelijk te manipuleren is. Vermelding van het sofinummer op de identiteitsbewijzen (paspoort, identiteitskaart, rijbewijs) heeft dus onbedoeld identiteitsfraude veel gemakkelijker gemaakt. Biometrie *op* het paspoort zal hetzelfde doen. De identiteitsfraudeur kan het biometrische kenmerk van het paspoort aflezen en vervolgens de identiteitscontrole foppen door dat kenmerk op het eigen lichaam aan te brengen of door een willekeurig ander kenmerk te gebruiken dat ongeveer dezelfde meetwaarde oplevert. Geen enkele biometrische techniek is op dit moment veilig op grote schaal te gebruiken. Het spelbederf van paspoortbiometrie in de vorm van een sterke toename van identiteitsfraude is dus een realistische verwachting.

Laten we voor ons model eens veronderstellen dat vermelding van het biometrische kenmerk *op* het paspoort leidt dan tot méér identiteitsfraude in plaats van tot minder. Hoe zou dat spelbederf mogelijk zijn? Dat plaatst ons voor de vraag, hoe we eigenlijk iemands identiteit (kunnen) controleren. In ieder geval niet met de gegevens die op het identiteitsbewijs staan! Wie door een identiteitscontrole heen wil glippen, kent die gegevens immers en kan er gemakkelijk op inspelen. Bovendien, voor identiteitsbewijzen en identiteitscontroles gelden in onze rechtstaat regels waardoor de identiteitsfraudeur in de huidige situatie goed kan voorspellen waar, wanneer, hoe en door wie zijn identiteit zal worden gecontroleerd. Identiteitscontroles zijn volgens de geldende regelgeving bovendien vaak openbaar en kunnen ongemerkt worden geobserveerd, op zoek naar zwakke plekken in techniek, organisatie of procedures. Behalve de geldende regelgeving vormen ook achterliggende rechtsnormen in onze rechtstaat een verklaring voor geritualiseerde identiteitscontroles, bijvoorbeeld de rechtsnorm dat men onschuldig is totdat het tegendeel bewezen is. Deze regel correspondeert met een algemene norm in onze rechtscultuur dat je voor achterdocht een gegronde reden moet hebben. Dat betekent, dat men doorgaans vindt dat men niet voortdurend alert mag zijn op identiteitsfraude. We moeten onze behoefte om iemands identiteit te controleren opzouten tot er een

serieus vermoeden rijst van kwade trouw. Maar dan is het meestal te laat: de identiteitsfraudeur is niet meer te vinden, of moet bij gebrek aan bewijs met rust worden gelaten. Zelfs de overheid mag zich zonder wettelijke regeling niet bedienen van procedures die iedereen verplichten zich te laten controleren vanuit een algemene achterdocht. Dat is zonder een dergelijke wettelijke regeling alleen rechtmatig als die controle op basis van vrijwilligheid geschiedt. En dat betekent weer, dat betrokkene vooraf op de hoogte moet worden gebracht. Het element van verrassing staat zodoende alleen ten dienste van de identiteitsfraudeur. Zo kan een identiteitsfraudeur met enige voorbereiding de meeste identiteitscontroles verschalken.

4. Paspoortbiometrie als dwarskijker

Als men wil weten hoe dit spelbederf kan worden beperkt, is een ander denkkader nodig dan de bestuurlijke benadering die het spelbederf heeft uitgelokt. Paspoortbiometrie als dwarskijker, dus. We kiezen in plaats van een bestuurlijke bijvoorbeeld een justitiële invalshoek, gericht op *bestrijding van identiteitsfraude*. De gangbare exclusieve aandacht voor het identiteitsbewijs moeten we laten varen.
We zoeken een andere vorm van identiteitscontrole. We beperken ons tot twee punten. We dienen in de eerste plaats controlevormen te ontwikkelen die rechtstreeks op de persoon gericht zijn. Dat kan bijvoorbeeld met vragen die alleen de juiste persoon correct kan beantwoorden. De overheid gebruikt die nog nauwelijks bij identiteitscontroles. In de tweede plaats moet de voorspelbaarheid van het proces van identiteitscontrole verminderen door meer variatie en meer alternatieve methoden. Men dient zich daarbij te realiseren, dat in een digitale omgeving de gecontroleerde het initiatief heeft, niet de controleur. Zonder dat de controleur dat in de gaten heeft, kan de gecontroleerde door eigen doen of nalaten er voor zorgen dat hij in een uitzonderingsprocedure komt, bijvoorbeeld door met een tikje met een hamer de chip op het paspoort onklaar te maken. Op dat moment kan hij de controleur voorgekookte en ter plaatse niet-controleerbare gegevens aanreiken die zijn identiteitsbewering aannemelijk lijken te maken.

De voorgenomen paspoortbiometrie blijkt zo een nuttige dwarskijker. Analyse van het spelbederf maakt duidelijk, dat identiteitscontroles *ook zonder inzet van biometrie* anders zouden moeten verlopen om een identiteitsfraudeur (in de ruime opvatting) te kunnen betrappen. Een biometrisch kenmerk kan daar wel bij helpen, maar natuurlijk niet als we dat eerst kenbaar op het identiteitsbewijs zetten, een aanpak die wél nuttig was voor de klassieke bestrijding van *document*fraude in een analoge wereld. Voor bestrijding van *identiteits*fraude werkt de vingerafdruk *op* het identiteitsbewijs averechts, omdat iemand door die na te maken of na te bootsen onopgemerkt door een identiteitscontrole kan komen. ICT moet de identiteitscontrole voor de gecontroleerde ook minder voorspelbaar maken. Men moet dus vaker rechtstreeks controleren of men van doen heeft met de *juiste* persoon, bijvoorbeeld met ketenspecifieke controlegegevens waarvan de meelifter niet op de hoogte kan zijn. Identiteitscontroles moeten voor de gecontroleerde dus zó onvoorspelbaar worden, dat hij van tevoren niet meer kan inschatten of, wanneer, waar en hoe hij tegen de lamp zal lopen.

Zo dwingt het ruim opgevatte fenomeen ‘identiteitsfraude’ ons tot een andere kijk op het gebruik van ICT voor identiteitscontrole. Voor de praktijk van identiteitscontrole moeten de bestuurlijke en justitiële denkkaders elkaar natuurlijk aanvullen, want bestrijding van identiteitsfraude mag niet leiden tot minder aandacht voor valse papieren. Het is verheugend te constateren dat de Nederlandse overheid recent uitdrukkelijk heeft besloten tot gebruik van achterliggende databanken die ook andere biometrische kenmerken bevatten dan welke op het identiteitsbewijs staan. Met andere biometrische kenmerken dan op het document staan vermeld, wordt de identiteitscontrole voor een meelifter minder voorspelbaar en de kans groter dat hij tegen de lamp loopt. Met de andere kan worden nagegaan of de vingerafdrukken op het document onveranderd zijn.

5. Conclusie

Dit voorbeeld illustreert dat het gepresenteerde strategische beoordelingsmodel nuttig kan zijn als gereedschap voor beleidsmakers en hun adviseurs. Het justitiële denkkader plaatst vraagtekens bij de harde koppelingen tussen identiteitsbewijs en biometrische kenmerk waar de gangbare bestuurlijke benadering op uitkomt. Pas als een identiteitsfraudeur niet meer van tevoren weet waar, wanneer en hoe hij tegen de lamp zal lopen, kan identiteitsfraude effectief worden aangepakt. Preventie en bestrijding van identiteitsfraude moeten het hebben van een gevarieerd gebruik van uiteenlopende ketengebonden biometriestelsels in combinatie met verschillende chipcards, sleutels, codes en persoonsnummers, zodat de voorspelbaarheid

van identiteitscontroles kan worden teruggedrongen. Een groter aantal van elkaar onafhankelijke biometriestelsels beperkt bovendien de waarde van een geslaagde aanval op een biometrisch kenmerk, waardoor dit ook minder aantrekkelijk wordt.

De hier ingebrachte alternatieve justitiële invalshoek is overigens niet de enige relevante invalshoek om ICT als dwarskijker te laten werken. Eerder heb ik ook laten zien, dat de keteninvalshoek dezelfde rol vervult[7]. Het lijkt mij juist een uitdaging om voor een concreet geval de meest zinvolle invalshoek(en) te ontdekken en de desbetreffende professionals te mobiliseren, ten einde inzet van ICT zo vroeg mogelijk vooral zijn voordelige vruchten te laten afwerpen.

Het voorbeeld van de paspoortbiometrie is ten slotte ook op inhoudelijke niveau interessant. Biometrische identiteitscontrole zal zonder twijfel een belangrijke rol in onze informatiesamenleving gaan vervullen, zowel voor het herkennen van personen als voor het administratief koppelen of afschermen van persoonsgegevens. Dat zal ertoe leiden, dat misbruik van biometrische kenmerken een belangrijke vorm van identiteitsfraude zal worden. Door de eisen van het internationale maatschappelijke verkeer zal men biometrie echter bij voorkeur wereldwijd willen standaardiseren. Daartoe moeten eventuele nationale biometriestelsels interoperabel zijn, d.w.z. in alle landen gebruikt kunnen worden. Dat betekent, dat de paspoortbiometrie de facto de wereldstandaard voor biometrie zou kunnen worden, tenzij bij elke concrete toepassing toch ketengebonden maatwerk wordt gerealiseerd door ook andere identiteitsinstrumenten te gebruiken. Het spelbederf van de paspoortbiometrie in de vorm van toenemende identiteitsfraude krijgt anders een grimmig internationaal perspectief.

---

1 Dit artikel is verschenen in: Privacy en Informatie (P&I), 9e jaargang, nummer 1 (februari 2006), pp. 14-17, Kluwer, Deventer, ISSN 1388-0241 Het is een verkorte versie van ICT, *Spelbederver of Dwarskijker?* dat eerder is verschenen in: Liber Amicorum '50 Jaar informatiesystemen 1978-2028' ter gelegenheid van het afscheid van prof. dr T.M. Bemelmans (A. Valstar en M. van Genuchten, red), Technische Universiteit Eindhoven, maart 2004

2 Prof. dr mr J. (Jan) H.A.M. Grijpink (1946) studeerde Economie (1969) en Rechten (1971) aan de Rijksuniversiteit Groningen. De doctorsgraad werd hem in 1997 door de Technische Universiteit Eindhoven verleend, op basis van zijn proefschrift Keteninformatisering. Hij is vanaf 1995 werkzaam als raadadviseur bij de directie Algemene Justitiële Strategie van het ministerie van Justitie met als werkterrein informatiestrategie. Van 1984 tot 1995 was hij verantwoordelijk voor de Justitieautomatisering. In maart 2004 werd hij benoemd tot (parttime) bijzonder hoogleraar Informatiekunde aan de faculteit Wiskunde en Informatica van de Universiteit Utrecht, mede ten behoeve van de faculteit der Rechtsgeleerdheid, met als leeropdracht Keteninformatisering in de Rechtstaat (zie www.cs.uu.nl/people/grijpink).

3 Deze vorm van ketenspecifieke communicatie heb ik uitgebreid beschreven in: Grijpink, J.H.A.M., "K*eteninformatisering*", Sdu Uitgevers, Den Haag, 1997 (ISBN 90 5409 131 2), "*Werken met keteninformatisering*", Sdu Uitgevers, Den Haag, 1999 (ISBN 90 5409 226 2) en "*Informatiestrategie voor ketensamenwerking*", Sdu Uitgevers, Den Haag, 2002 (ISBN 90 1209 697 9).

4 Grijpink, J.H.A.M., "Identiteitsfraude als uitdaging voor de rechtstaat", Privacy & Informatie, 6e jaargang, nummer 4 (augustus), 2003, pp. 148-153, Koninklijke Vermande, Lelystad, ISSN 1388-0241

5 Grijpink, J.H.A.M., "Biometrie en privacy", Privacy & Informatie, 3e jaargang, nummer 6 (december), 2000, pp. 244-250, Koninklijke Vermande, Lelystad, ISSN 1388-0241

6 Grijpink, J.H.A.M., "Persoonsnummers en privacy", Privacy & Informatie, 5e jaargang, nummers 2 (april), pp. 52-56 en 3 (juni), 2002, pp. 100-105, Koninklijke Vermande, Lelystad, ISSN 1388-0241

7 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", Proceedings of the IS&T/SPIE 16th Annual Symposium 18-22 January 2004, San Jose, California USA, paper 5310-10